Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE: BALANCING TECHNOLOGICAL INNOVATION AND PERSONAL DATA PROTECTION RIGHTS. A COMPARATIVE LEGAL STUDY BETWEEN THE EUROPEAN UNION AND VIETNAM

Phuong Anh Nguyen

ABSTRACT

Background: *The rapid development of Artificial Intelligence has profoundly transformed various aspects of social life, including the criminal justice system. In criminal proceedings, the collection and processing of biometric, behavioural, and emotional data may threaten the right to privacy, the presumption of innocence, and the right to a fair trial. This study examines the intersection between technological innovation and personal data protection in criminal justice through a comparative legal analysis of the European Union and Vietnam. By analysing the EU's GDPR, Law Enforcement Directive, and AI Act 2024 alongside Vietnam's legal framework, the paper identifies key areas of convergence, divergence, and regulatory gaps.*

DOI:

https://doi.org/10.33327/AJEE-18-8.S-r000161

Date of submission: 26 Oct 2025
Date of acceptance: 08 Dec 2025
Online First publication: 19 Dec 2025
Last Published: 30 Dec 2025

Disclaimer:

The author declares that their opinion and views expressed in this manuscript are free of any impact of any organizations.

Methods: *The study employs comparative legal analysis, combined with a human rights–based approach, to clarify the relationship between technological innovation and the right to personal data protection in criminal justice. The sources of reference include the legal frameworks of the European Union and Vietnam, case law, and reports from EU and United Nations bodies.*

Results and Conclusions: *The study aims to establish fundamental legal principles that balance technological innovation with the protection of the right to personal data in criminal justice—an approach that has received limited attention in Vietnam. Based on this foundation, it proposes legal reforms toward a framework of "human rights–oriented digital justice", ensuring that the digitalisation and application of AI in the justice system not only enhance operational efficiency but also strengthen the rule of law and protect people.*

1 INTRODUCTION

The rapid development of Artificial Intelligence (AI) is creating profound changes in criminal justice activities worldwide. In many countries, AI tools have been tested or deployed at various stages of criminal proceedings—such as investigation, prosecution, and adjudication — to improve the efficiency of legal proceeding activities, while minimising "unintentional" or "intentional" errors made by humans. These technologies assist competent authorities in making judicial decisions more quickly, transparently, and objectively. Such efforts not only reflect the trend of modernising the justice systems but also represent the broader digital revolution that is reshaping how the State exercises judicial power in the 21st century.[1] However, alongside the opportunity for innovation, AI technologies also expose an increasingly clear contradiction between two fundamental legal objectives: technological innovation in judicial activities and the protection of human rights, particularly the right to data protection. AI governance, therefore, cannot only remain at the level of ethical recommendations; it must be firmly grounded in the rule of law. AI should be guided to serve human development rather than merely optimise efficiency.[2] This reality underscores the urgent need to integrate human values, accountability, and transparency into the justice system's digital transformation.

The EU is a pioneer in establishing a legal framework that balances technological innovation and personal data protection. The Artificial Intelligence Act (AI Act) of 2024 is the first legal document in the world to comprehensively regulate AI based on a risk-classification approach, in which applications in the fields of justice and law enforcement are categorised

[1] Angela Daly and others, 'Artificial Intelligence, Governance and Ethics: Global Perspectives' (Research Paper no 2019-15, The Chinese University of Hong Kong Faculty of Law 2019) doi:10.2139/ssrn.3414805.

[2] Bernd Carsten Stahl and others, 'Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning' (2021) 124 Journal of Business Research 374. doi:10.1016/j.jbusres.2020.11.030.

as "high-risk."[3] Alongside this, the Directive 2016/680/EU[4] (Law Enforcement Directive – LED) and the Regulation 2016/679/EU[5] (General Data Protection Regulation – GDPR) reaffirm the position of "the right to personal data protection" as a fundamental right, guaranteed in all data processing activities conducted for criminal proceedings.

In Vietnam, digital transformation in judicial activities has been institutionalised through a series of policies and legal documents. Resolution No. 27-NQ/TW of the Central Committee of the Communist Party of Vietnam[6] affirms the requirement to modernise judicial activities and apply new technologies while simultaneously respecting and protecting human rights. The 2015 Criminal Procedure Code for the first time recognises electronic data as a source of evidence (Articles 87 and 99),[7] paving the way for the application of information technology and AI in collecting, evaluating, and using evidence. Furthermore, Decree No. 13/2023/ND-CP on personal data protection[8] and the 2025 Law on Personal Data Protection[9] (effective from 1 January 2026) have established a unified legal foundation to protect individual rights in the digital space. However, as judicial authorities begin to utilise big data, biometrics, and AI-powered predictive analytics tools, a crucial question arises: how can new technologies be applied without "diminishing" the level of protection of fundamental human rights, especially the right to personal data protection?

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act - AI Act) <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 24 October 2025.

[4] 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 (Law Enforcement Directive - LED) [2016] OJ L 119/89.

[5] 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 (General Data Protection Regulation - GDPR) [2016] OJ L 119/1.

[6] Resolution of the Central Committee of the Communist Party of Vietnam No 27-NQ/TW 'On Continuing to Build and Perfect the Socialist Rule of Law State of Vietnam in the New Period' (9 November 2022) [in Vietnamese] <https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Nghi-quyet-27-NQ-TW-2022-tiep-tuc-xay-dung-Nha-nuoc-phap-quyen-xa-hoi-chu-nghia-giai-doan-moi-541092.aspx> accessed 24 October 2025.

[7] Law of the Socialist Republic of Vietnam No 101/2015/QH13 'Criminal Procedure Code' (27 November 2015) <https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-to-tung-hinh-su-2015-296884.aspx> accessed 24 October 2025.

[8] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP 'Protection of Personal Data' (17 April 2023) <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx> accessed 24 October 2025.

[9] Law of the Socialist Republic of Vietnam No 91/2025/QH15 'Personal Data Protection' (26 June 2025) <https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx> accessed 24 October 2025.

Based on the practice of the EU and Vietnam, this study focuses on clarifying: (i) the theoretical framework and legal principles governing the relationship between AI and personal data in criminal proceedings; (ii) the EU's experience and balancing mechanism as reflected in typical legal documents and case law; and (iii) suggestion for improving Vietnamese law to ensure that technological innovation is aligned with the protection of the right to personal data. This study not only systematises Vietnam's legal framework amid the digital transformation of justice but also proposes a balanced model in which technological innovation and personal data protection reinforce one another to build a modern, humane, and trustworthy criminal justice system.

2 METHODOLOGY

The article adopts the doctrinal legal research method combined with comparative legal analysis, grounded in a human rights–based approach. The EU is one of the most successful regions in the world in establishing both a comprehensive legal framework and effective mechanisms for the protection of human rights in general and of personal data in particular. For this reason, the author has chosen the EU model as a good-practice example to analyse and draw relevant lessons for improving Vietnam's legal framework in this field. To achieve this objective, the research sources include legal documents of the EU, including the GDPR, Law Enforcement Directive (LED), AI Act, and Convention 108+, and related legal documents of Vietnam, along with the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). This methodology aims to explain, compare, and generalise key legal principles, especially the principles of lawfulness, necessity, and proportionality, as well as accountability in the application of AI in criminal justice. The article does not use empirical data; rather, it focuses on normative analysis and academic arguments, thereby providing directions for improving the law and policy implications tailored to Vietnam's context.

3 CONCEPT FRAMEWORK

3.1. The Definition of "Artificial Intelligence in Criminal Justice"

In legal science, there is no absolute unified definition of AI. However, within the European legal framework, the commonly adopted understanding of AI is a system capable of "reasoning, learning, and generating predictions, recommendations, or decisions that may affect real or virtual environments" based on the analysis of pre-programmed input data.[10]

[10] EU-LISA and Eurojust, *Artificial Intelligence Supporting Cross-Border Cooperation in Criminal Justice* (Publications Office of the EU 2022). doi:10.2857/364146.

In the context of criminal justice, AI refers to the use of fully or semi-automated digital systems to assist humans with procedural activities such as collecting, analysing, and evaluating evidence; managing case files; forecasting the risk of recidivism; or monitoring the execution of sentences. The goal of applying AI is to enhance the efficiency of crime detection and handling while reducing the workload of judicial and prosecutorial authorities.

However, as these activities directly affect individual freedoms and the right to a fair trial, the application of AI in the criminal justice system must always be subject to strict legal limits and human oversight. Since AI systems used in law enforcement and criminal justice are classified as "high-risk", they are subject to additional obligations, such as assessing conformity, record-keeping, ensuring transparency and explainability of outputs, and "human oversight," which means humans must always retain ultimate control.[11]

3.2. The Definition of "Technological Innovation in Criminal Justice"

The concept of technological innovation in criminal justice not only refers to the adoption of new technologies but also implies a fundamental transformation in the process of exercising judicial authority. From an academic perspective, technological innovation in this field can be identified through three key legal criteria:

First, the degree of automation and its impact on procedural decisions. The more capable the system is of making decisive conclusions or suggestions (for example: analysing DNA samples, recognising a suspect's facial features, or recommending sentencing based on precedent data), the higher the legal requirements regarding transparency, explainability, and verifiability.[12]

Second, the type of data being processed. In the field of criminal justice, most data is classified as sensitive, especially biometric, health, and personal data, as well as information concerning political or religious beliefs. According to the EU Directive 2016/680 on data protection in law enforcement activities (the Law Enforcement Directive – LED), the processing of such data is lawful only if there is a clear legal basis that complies with the principles of necessity and proportionality.[13]

Third, the legal consequences for human rights. Every application of technology in criminal proceedings must be assessed through the lens of the right to a fair trial, the right to privacy, and the right to personal data protection. The use of surveillance or predictive analysis tools without adequate safeguards and legal boundaries may pose risks of human rights violations. The European Court of Human Rights, in *S. and Marper v. the United Kingdom* (2008), affirmed that the indefinite and indiscriminate retention of biometric

[11] Regulation (EU) 2024/1689 (n 3).

[12] ibid

[13] Directive (EU) 2016/680 (n 4).

data from individuals who have not been convicted of a crime is a disproportionate interference with the right to respect for private life under Article 8 of the European Convention on Human Rights.[14]

3.3. The Definition of "Right to Personal Data Protection in Criminal Justice"

The right to personal data protection has a solid foundation in international human rights law. According to provisions in Article 12 of the Universal Declaration of Human Rights (1948),[15] Article 17 of the International Covenant on Civil and Political Rights (1966),[16] and Article 8 of the European Convention on Human Rights (1950),[17] it can be seen that the principles of lawfulness, necessity, and proportionality must govern the collection, storage, and use of personal information. In particular, the development of Convention 108+ (2018) has held that the "right to personal data protection" is an independent right, closely linked to the "right to privacy".[18] This represents a new generation of fundamental human rights designed to address the challenges posed by the era of AI and big data.

In the criminal field, Directive 2016/680/EU establishes a distinct protection mechanism for the processing of personal data by competent authorities for investigation, prosecution, and adjudication. It allows for certain restrictions of individual rights, such as the right to access or object, but only to the extent necessary to avoid obstructing judicial activities. At the same time, it requires the establishment of independent monitoring mechanisms and guarantees effective rights to appeal.[19]

In Vietnam, this right has recently been institutionalised by Decree No. 13/2023/ND-CP and the 2025 Law on Personal Data Protection. These documents set forth seven fundamental principles governing the processing of personal data, including "collecting data only as necessary for legitimate purposes", "ensuring the accuracy and timeliness of data", and "retaining data only for the necessary period".[20] The 2025 Law on Personal Data Protection further reaffirms the fundamental rights of data subjects and

[14] *S and Marper v the United Kingdom* Apps nos 30562/04, 30566/04 (ECtHR, 4 December 2008) <https://hudoc.echr.coe.int/fre?i=001-90051> accessed 24 October 2025.

[15] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217A) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 24 October 2025.

[16] International Covenant on Civil and Political Rights (adopted 16 December 1966 UNGA Res 2200A(XXI)) 999 UNTS 171.

[17] Council of Europe, *European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols)* (ECHR 2013).

[18] Council of Europe, *Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (Council of Europe 2018) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 24 October 2025.

[19] Directive (EU) 2016/680 (n 4).

[20] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP (n 8); Law of the Socialist Republic of Vietnam No 91/2025/QH15 (n 9).

establishes a mandatory Data Protection Impact Assessment (DPIA) mechanism for data processing activities that pose a risk of infringing on privacy rights, particularly in the fields of justice and law enforcement.

When AI is integrated into this process, from facial recognition and behavioural analysis to risk prediction, personal data becomes not only a tool for investigation but also central to the right to a fair trial and the principle of the presumption of innocence.[21] The application of AI in criminal justice must therefore be framed within the context of human rights, ensuring that all technological innovations adhere to the principles of lawfulness, necessity, proportionality, human supervision, and accountability, to prevent the automation of judicial power.[22] In this context, the Fundamental Rights Impact Assessment (FRIA) serves as a core legal instrument in AI governance, helping to balance technological innovation and the protection of personal data rights, particularly in investigation and adjudication activities.[23] This demonstrates that a human rights–based model of criminal justice is the most appropriate approach to harmonise technological innovation with the safeguarding of personal data protection.

Therefore, the right to personal data protection in criminal justice is not only an extension of the right to privacy in the digital environment, but also a legal instrument to ensure control over state power when applying AI in investigation, prosecution, and adjudication. This right serves both preventive and protective functions, aiming to maintain a balance between technological efficiency and human rights protection. On that basis, it is essential to establish a set of fundamental legal principles to guide all activities in designing, implementing, and monitoring judicial technologies. This helps ensure that innovation occurs within the rule of law and in conformity with international human rights standards.

4 KEY PRINCIPLES ENSURING A BALANCE BETWEEN TECHNOLOGICAL INNOVATION AND THE RIGHT TO PERSONAL DATA PROTECTION

4.1. The Principles of Lawfulness, Necessity, and Proportionality

The principles of lawfulness, necessity, and proportionality were developed and refined through the case law of the European Court of Human Rights (ECtHR) in its interpretation

[21] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review 494.

[22] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) Computer Law & Security Review 754. doi:10.1016/j.clsr.2018.05.017.

[23] Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020. doi:10.1016/j.clsr.2024.106020.

of Article 8 of the European Convention on Human Rights (ECHR). A series of cases, from *S. and Marper v. the United Kingdom,*[24] *Uzun v. Germany,*[25] *Roman Zakharov v. Russia*[26] *to Big Brother Watch and Others v. the United Kingdom*[27] has established a three-tier standard in interpreting Article 8 ECHR, consisting of: (i) lawfulness – any interference must have a clear and foreseeable legal basis; (ii) necessity – it must only be applied in a democratic society; and (iii) proportionality – the degree of interference must not exceed what is required to protect the public interests. Among these cases, *S. and Marper v. the United Kingdom* represents a pivotal and foundational case, in which the ECtHR affirmed that the indefinite retention of biometric data of individuals who have not been convicted is an "unjustified interference with the right to privacy", thereby violating Article 8 of the European Convention on Human Rights.[28]

In EU laws, the principle of proportionality has been elevated to a constitutional legal standard and has been institutionalised in legal documents governing emerging technologies, most notably the 2024 AI Act. According to Article 6 and Annexe III of this document, AI systems used in law enforcement, investigation, prosecution, adjudication, and the execution of sentences are classified as high-risk.[29] To be deployed, such systems must comply with a set of mandatory legal obligations, including ex ante risk assessment, ensuring transparency, explainability, and human supervision, as well as the post-market monitoring mechanisms to control the entire lifecycle of the system.

In Vietnam, although the principles of lawfulness, necessity, and proportionality have not yet been explicitly defined in the field of AI, the key elements of these principles are indirectly reflected in Decree No. 13/2023/ND-CP and the 2025 Law on Personal Data Protection. According to Article 3 of Decree No. 13/2023/ND-CP, the processing of personal data must adhere to the principles of "only collecting data within the scope necessary for legitimate purposes", ensuring that data are "up to date," and "only retaining data for the necessary period".[30] In particular, the 2025 Law on Personal Data Protection adds the obligation to conduct a Data Protection Impact Assessment (DPIA) for data processing and transfer activities, including the application of AI in investigation, prosecution, and adjudication.[31] Although Vietnam has not yet adopted a Fundamental Rights Impact Assessment (FRIA) mechanism like the EU's, the DPIA represents an important step toward integration and toward balancing technological innovation and human rights.

[24] *S and Marper* (n 14).

[25] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010) <https://hudoc.echr.coe.int/eng?i=001-100293> accessed 24 October 2025.

[26] *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) <https://hudoc.echr.coe.int/fre?i=001-159324> accessed 24 October 2025.

[27] *Big Brother Watch and Others v the United Kingdom* Apps nos 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 2021) <https://hudoc.echr.coe.int/eng?i=001-210077> accessed 24 October 2025.

[28] *S and Marper* (n 14).

[29] Regulation (EU) 2024/1689 (n 3).

[30] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP (n 8).

[31] Law of the Socialist Republic of Vietnam No 91/2025/QH15 (n 9).

4.2. The Principle of Accountability and Impact Assessment

According to Article 5(2) of the General Data Protection Regulation 2016/679 (GDPR), data controllers are responsible for, and must be able to demonstrate, compliance with the data protection principles.[32] This responsibility is operationalised through the Data Protection Impact Assessment (DPIA), a preventive tool designed to identify and mitigate risks before technology is applied. The obligation to conduct a DPIA is stipulated in Article 35 of the GDPR and Article 27 of Directive 2016/680 (LED), requiring an assessment of any data processing activities that pose a high risk, including the use of new technologies or large-scale monitoring.[33]

Accountability and impact assessment mechanisms are ethical and legal tools that enable the state and public authorities to balance technological innovation with the protection of human rights, thereby establishing a Human Rights, Ethical, and Social Impact Assessment (HRESIA) framework for high-risk AI systems.[34] In the context of criminal proceedings, these tools are particularly essential for controlling the transparency, accuracy, and bias of AI systems used in investigation, adjudication, or risk assessment. In the case of *State v. Loomis,* the defendant was sentenced based on the results of the COMPAS software but was unable to challenge or verify the algorithm, providing a clear example of the risks of algorithmic justice.[35] In Europe, in *NJCM v. the Netherlands*, the Hague Court also held that the government's use of a risk prediction system without a DPIA and an independent accountability mechanism violated Article 8 of the ECHR.[36] The Court affirmed that a human rights impact assessment procedure must govern all AI applications in the public sector.

Vietnamese law has adopted a similar approach. Decree No. 13/2023/ND-CP establishes an obligation to conduct impact assessments for high-risk data processing activities, particularly in the areas of security, justice, and information technology.[37] Subsequently, the 2025 Law on Personal Data Protection sets out mechanisms for reporting, independent monitoring, and the accountability of state agencies in managing personal data.[38] This represents an important step toward establishing a risk control mechanism for data in criminal proceedings. However, Vietnam is currently only at the internal assessment stage and lacks an independent, transparent accountability mechanism similar to the EU's DPIA-FRIA model.

[32] Regulation (EU) 2016/679 (n 5).

[33] ibid; Directive (EU) 2016/680 (n 4).

[34] Mantelero (n 22; 23).

[35] *State v Loomis* 371 Wis.2d 235, 881 N.W.2d 749 [2016] Wisconsin Supreme Court <https://case-law.vlex.com/vid/state-v-loomis-no-888404547> accessed 24 October 2025.

[36] *NJCM c The Netherlands C-09-550982-HA ZA 18-388* [2020] Rechtbank Den Haag ECLI:NL:RBDHA:2020:1878 <https://www.escr-net.org/wp-content/uploads/2020/09/ecli_nl_rbdha_2020_1878.pdf> accessed 24 October 2025.

[37] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP (n 8).

[38] Law of the Socialist Republic of Vietnam No 91/2025/QH15 (n 9).

4.3. The Principle of Transparency and Human Supervision

According to Article 14 and Annexe III of the 2024 AI Act, high-risk AI systems, including tools used in law enforcement and criminal proceedings, must be equipped with "human supervision", meaning that humans can supervise, intervene, or suspend the system's processing when necessary.[39] This obligation is not only technical but also reflects the principle of the rule of law: humans remain the ultimate decision-makers in the judicial process, thereby maintaining the legitimacy of state authority in the digital era.

The report *Human Rights Due Diligence for Digital Technology Use* published by the United Nations Office of the High Commissioner for Human Rights (OHCHR) emphasises that all government agencies employing digital or AI systems must conduct human rights impact assessments, ensure transparency regarding the purpose and operation mechanisms, and maintain human supervision throughout the technology's lifecycle, especially in areas that may affect personal freedoms, dignity, and the right to access to justice.[40] Similarly, both the OECD AI Principles[41] (issued in 2019 and updated in 2024) and the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law[42] (2024) require countries to ensure that humans remain the ultimate responsible party. Humans should be able to intervene, suspend, or disable AI systems when there is a risk of human rights violations. These documents reflect a global shift from "autonomous AI" to "AI for people", aiming to maintain transparency, accountability, and the rule of law in all areas, particularly in criminal justice, where the impacts of technological decisions can directly affect individuals' fates and personal freedoms.

In Vietnam, although there has not been a legal document directly governing the use of AI in legal proceedings, the 2015 Criminal Procedure Code contains provisions that lay the foundation for control, such as Article 8 (guaranteeing human rights) and Article 99 (on the evidentiary value of electronic data).[43] These provisions provide a legal basis for controlling the evidentiary value of electronic data, including outputs from AI systems. Accordingly, all evidence must be collected, examined, and assessed in accordance with legal procedures, meaning that AI cannot automatically become a valid source of evidence without human verification. This approach reflects the spirit of the "human supervision" principle and ensures that the digitisation of justice maintains transparency, fairness, and humanity – the core values of the rule of law state.

[39] Regulation (EU) 2024/1689 (n 3).

[40] OHCHR, 'Human Rights Due Diligence for Digital Technology Use - Guidance of the Secretary-General: Practical Guide' (*United Nations Human Rights*, 30 September 2025) <https://www.ohchr.org/en/documents/tools-and-resources/human-rights-due-diligence-digital-technology-use-guidance> accessed 24 October 2025.

[41] OECD, 'AI Principles' (2024) <https://www.oecd.org/en/topics/sub-issues/ai-principles.html> accessed 24 October 2025.

[42] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (5 September 2024) CETS 225 <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> accessed 24 October 2025.

[43] Law of the Socialist Republic of Vietnam No 101/2015/QH13 (n 7).

4.4. The Principle of a Balanced Approach in Applying AI to Criminal Justice

The "balance" in the application of AI to criminal justice is not merely about finding a middle ground between technological efficiency and the protection of human rights, but rather a dynamic legal mechanism that ensures the values of the rule of law are maintained throughout the innovation process.[44] Balance is understood as a continuous legal balancing process, in which each stage of the proceedings (investigation, prosecution, trial, and enforcement) must be re-evaluated for the lawfulness, necessity, and proportionality of applying new technologies, over time and in specific contexts.[45]

The concept of dynamic balance originates from how the European Court of Human Rights (ECtHR) interprets Article 8 of the European Convention on Human Rights (ECHR) with the criteria of lawfulness, necessity, proportionality, and the "fair balance". In the case of *S. and Marper v. the United Kingdom*, the ECtHR considered the comprehensive and indefinite retention of biometric data from individuals not convicted of a crime to be unnecessary in a democratic society due to the lack of time limits and insufficient safeguards.[46] This implies that the level of intervention must be flexible in response to technological risks and be subject to periodic review. In *Big Brother Watch and Others v. the United Kingdom,* the ECtHR demanded "end-to-end safeguards" (including selection criteria, independent approval, and continuous monitoring) for mass data collection,[47] indicating that proportionality is not static but evolves alongside the risks and the intensity of actual monitoring.[48]

The EU's 2024 AI Act incorporates this concept into law through a lifecycle, risk-based governance model: "high-risk" AI systems in law enforcement and judicial operations must undergo periodical assessments, ensure transparency and explainability, and maintain "human supervision."[49] This means that humans have the authority to intervene, adjust, or suspend the system's operation when necessary. Simultaneously, the Council of Europe's AI Framework Convention requires countries to maintain a risk-based and rights-based balancing mechanism with safeguards throughout the entire lifecycle, thereby establishing a "dynamic balance" standard that encourages innovation without exceeding the boundaries of human rights and the rule of law.[50]

[44] Jonida Milaj, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2016) 30(3) International Review of Law, Computers & Technology 115. doi:10.1080/13600869.2015.1076993.

[45] Mantelero (n 22; 23).

[46] *S and Marper* (n 14).

[47] *Big Brother Watch and Others* (n 27).

[48] Kristina Trykhlib, 'The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights' (2020) 4 EU and Comparative Law Issues and Challenges Series (ECLIC) 128. doi:10.25234/eclic/11899.

[49] Regulation (EU) 2024/1689 (n 3).

[50] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (n 42).

In Vietnam, the principle of balance has started to emerge within the personal data protection framework. Decree 13/2023/ND-CP requires data processing to be purpose-driven, minimized, and subject to retention limits, while the 2025 Personal Data Protection Law establishes impact assessments for high-risk activities - requirements that can be directly integrated into each stage of legal proceedings to repeatedly verify the lawfulness, necessity, and proportionality of using AI.[51] Combined with Articles 8 and 99 of the 2015 Criminal Procedure Code,[52] a dynamic balancing mechanism can be designed on a case-by-case and time-bound basis to ensure that AI is a controlled support tool, not a replacement for human judicial judgment.

5 THE EU'S EXPERIENCE IN ENSURING THE BALANCE BETWEEN TECHNOLOGICAL INNOVATION AND PERSONAL DATA PROTECTION IN CRIMINAL JUSTICE

5.1. The EU's Legal Framework for Ensuring the Balance between Technological Innovation and Personal Data Protection

The experience of the EU shows that ensuring the balance between technological innovation and personal data protection is underpinned by a multi-layered legal framework, in which the principles of human rights and technological innovation are consistently integrated at the constitutional level. The European Union Charter of Fundamental Rights recognises the right to personal data protection as an independent right (Article 8),[53] which forms the foundation for the GDPR, LED, and AI Act– three legal pillars that directly regulate the relationship between technology and human rights in the field of criminal justice.

(i) The GDPR establishes core principles for data processing, including: lawfulness, transparency, purpose limitation, data minimisation, and accountability. Articles 5(2) and 35 of the GDPR require conducting a DPIA for high-risk activities, especially when applying new technologies in investigations or adjudication.[54]

(ii) The Directive (EU) 2016/680 (LED) extends the principles of GDPR to the criminal field, allowing flexibility in restricting certain rights (such as the right to access or object) when necessary for the proceedings. But it still requires the principles of lawfulness, necessity, proportionality, and independent oversight mechanisms.[55]

[51] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP (n 8); Law of the Socialist Republic of Vietnam No 91/2025/QH15 (n 9).

[52] Law of the Socialist Republic of Vietnam No 101/2015/QH13 (n 7).

[53] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[54] Regulation (EU) 2016/679 (n 5).

[55] Directive (EU) 2016/680 (n 4).

(iii) The AI Act marks a new step in EU law by treating AI systems in the judicial, law enforcement, and national security fields as a "high-risk" group. The AI Act requires these systems to comply with transparency, training data governance, periodic risk assessments, and human oversight mechanisms, ensuring that judicial decisions are not "automated" but remain subject to human control.[56]

The three abovementioned documents do not stand separately but operate as mutually reinforcing normative layers, forming a dynamically balanced legal mechanism in which technology is developed within the framework of human rights and the rule of law. This system helps the EU to shift its approach from "protection against technology" to "responsible technological governance". The EU does not consider the right to personal data protection as a barrier but a necessary condition for legitimate and sustainable innovation. Based on that legal foundation, the EU has developed numerous enforcement and monitoring mechanisms to maintain a balance between technological innovation and human rights in judicial practice, especially at the member-state level.

5.2. Balancing Mechanisms through Impact Assessment and Risk Control

Based on the multi-layered legal framework established at the Union level, the EU has developed a series of preventive and adaptive enforcement mechanisms to maintain the balance between technological innovation and human rights protection throughout the entire lifecycle of data and AI systems. The focus of this mechanism lies in impact assessment and risk control—legal tools that help translate abstract human rights principles into concrete, measurable, and monitorable operational procedures in judicial practice.

A highlight of the EU experience is the prevention of legal risks and the protection of human rights from the technological design stage. It is based on the principle that innovation is legitimate only when carried out within predictable, controllable limits, ensuring that human rights are not compromised for the sake of efficiency.[57] According to Article 35 of the GDPR, data controllers must conduct a data protection impact assessment (DPIA) where processing activities are "likely to pose a high risk" to the rights and freedoms of individuals, in particular where "systematic surveillance on a large scale" or "new technologies are applied".[58] DPIA is not only a technical procedure, but a legal balancing mechanism that requires data processors to anticipate, model, and mitigate risks before deploying technology.

[56] Regulation (EU) 2024/1689 (n 3).

[57] EDPS, 'Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (24 October 2025) <https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures> accessed 24 October 2025.

[58] Regulation (EU) 2016/679 (n 5).

In the field of justice and security, Directive (EU) 2016/680 (LED) specifies this mechanism in Articles 27 – 31.[59] It requires competent authorities to clearly define the legal basis for the collection, processing, and storage of data, to ensure that the processing purposes are clearly defined and that the storage period does not exceed the needs of the investigation, prosecution, or adjudication. LED also demands the establishment of an independent monitoring system led by the national data protection authority. This is an ex post control mechanism that helps maintain the balance between judicial power and the legal framework, ensuring the rule of law.

The combination of ex ante and ex post control creates a continuous balancing cycle in the governance of judicial technology. This approach is reinforced by the Court of Justice of the European Union (CJEU) through case law. Typically, in *Digital Rights Ireland Ltd. v. Minister for Communications*, CJEU held that the indiscriminate retention of telecommunications data from all citizens violates the principle of proportionality, as there are no clear limits on the scope, duration, and mechanism of access to the data.[60] Subsequently, *Tele2 Sverige AB v. Watson* affirmed that any data monitoring mechanism must be based on "objective criteria" and "independent prior review", thereby establishing a new legal standard for controlling technological risks in the justice sector.[61] Case law is fundamental to the entire EU legal framework on AI and data in the justice sector.

Thus, the EU model does not concentrate on "preventing" technology, but on creating a legal framework for responsible innovation. DPAI, FRIA, and the independent monitoring mechanism are not only technical tools but also institutional manifestations of the principles of balancing judicial efficiency and the protection of human rights—an important experience for Vietnam in perfecting the legal framework for applying AI in criminal proceedings.

5.3. Enforcement Mechanism and the Role of Independent Monitoring Bodies

If the principles of lawfulness, necessity, and proportionality establish "theoretical standards" for data processing, then enforcement mechanisms and independent monitoring bodies serve to ensure these standards are implemented effectively, transparently, and verifiably. In the EU system, this enforcement structure is designed based on three complementary pillars: (i) an independent monitoring body with substantive enforcement powers; (ii) a technical–legal oversight mechanism along the life cycle of high-risk

[59] Directive (EU) 2016/680 (n 4).

[60] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECJ ECLI:EU:C:2014:238 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293> accessed 24 October 2025.

[61] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECJ ECLI:EU:C:2016:970 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203> accessed 24 October 2025.

technologies; and (iii) a unified coordination mechanism across the Union to maintain common rule of law standards.

(1) *Independent monitoring body – the heart of the balancing mechanism.* This principle was established in the case of Commission v. Germany, in which the CJEU held that any government intervention in the activities of a data protection authority violates the duty of absolute independence.[62] This was reinforced in the Schrems II case, where the Court stressed that the monitoring authority must be able to proactively suspend data processing when there is a risk of a fundamental right being violated.[63] This provision is codified in Article 52 GDPR and Article 41 LED, requiring Data Protection Authorities (DPAs) to have organisational autonomy, budget, and enforcement powers.

(2) *Lifecycle technical oversight mechanism – ensuring balance in the innovation process.* To ensure consistency and implementation, the European Commission has established the AI Office. This agency has the authority to request that AI developers provide technical dossiers, testing information, incident reports, and evidence of human oversight to ensure compliance with the obligations under the AI Act.[64] This mechanism shifts the concept of "balance" from a static state to a dynamic one, in which all AI applications in the justice sector are not only approved once but also periodically reviewed as technology and risk levels evolve. This is a manifestation of evolutionary balance, in which the legality and the protection of human rights of the technology are continuously re-examined throughout its operational lifecycle.

(3) *Union-wide consistency and coordination mechanism – ensuring systemic balance.* In addition to national oversight, the EU has established a consistency mechanism to maintain uniformity in data protection. Under Articles 63 – 65 of the GDPR, if DPAs have different views on a cross-border case, the European Data Protection Board (EDPB) can issue a binding decision that the parties must comply with.[65] This mechanism creates horizontal balance among Member States, prevents legal fragmentation, and ensures that all individuals in the EU enjoy equal protection from technology-related risks, irrespective of their residence or the location of data processing.

[62] *Uzun v Germany* (n 25).

[63] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems II* [2020] ECJ ECLI:EU:C:2020:559 <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=ecli:ECLI:EU:C:2020:559> accessed 24 October 2025.

[64] 'European AI Office' (*European Commission: Shaping Europe's Digital Future*, 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-office> accessed 24 October 2025.

[65] EDPB, 'Guidelines 03/2021 on the Application of Article 65(1)(a) GDPR' (adopted 13 April 2021) <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-032021-application-article-651a-gdpr_en> accessed 24 October 2025.

In the field of criminal justice, the three-layered mechanism has profound legal implications. The combination of independent oversight and technical monitoring ensures that procedural efficiency cannot be achieved at the expense of human rights. This approach allows the EU to implement the principle of "justice must not be automated": technology can assist in judgment, but only humans can make the final judicial decisions.

The above comparison shows that the main differences lie in institutional standardisation and risk-governance mechanisms. The EU has developed a three-tier legal framework (GDPR, LED, AI Act) with independent oversight, while Vietnam is still forming its basic structure, lacking both an independent data authority and mandatory impact assessments. The EU's experience offers guidance for Vietnam to balance innovation with human rights protection in criminal justice. Although the EU is regarded as a pioneering jurisdiction in data protection and technological risk governance, its model also has limitations, such as the implementation of the 2024 AI Act, which has generated debate over its enforceability, particularly given the significant differences in infrastructure readiness and supervisory capacity among Member States. In addition, the Schrems II judgment[66] showed that the EU continues to face difficulties in ensuring cross-border data security and maintaining consistent standards with international partners. These limitations indicate that the EU's experience does not constitute a "perfect model," but rather serves as a reference point for Vietnam as it develops a balanced mechanism suited to its national context.

6 LEGAL STATUS AND CHALLENGES IN VIETNAM IN ENSURING A BALANCE BETWEEN TECHNOLOGICAL INNOVATION AND PERSONAL DATA PROTECTION IN CRIMINAL JUSTICE

The process of digital transformation in the justice sector in Vietnam creates many opportunities for innovation, but also poses an urgent need to ensure a balance between technological efficiency and the right to protect personal data. Although the fundamental legal framework, such as the 2015 Criminal Procedure Code, Decree 13/2023/ND-CP, and the 2025 Law on Personal Data Protection, has been issued, the current legal system still lacks a mechanism to incorporate, monitor, and control technological risks in criminal justice.

6.1. Current Status of Vietnamese Laws

The 2015 Criminal Procedure Code, for the first time, recognises electronic data as a source of evidence (Articles 87 and 99) and allows the use of digital means in the process of collecting, examining, and evaluating evidence.[67] This provision marked a turning point, shifting from traditional to digital thinking in litigation and paving the way for the

[66] Case C-311/18 (n 63).

[67] Law of the Socialist Republic of Vietnam No 101/2015/QH13 (n 7).

integration of automated analysis tools and decision-support systems in investigation, prosecution, and adjudication. Additionally, Decree No. 13/2023/ND-CP on Personal Data Protection and the 2025 Law on Personal Data Protection (effective from 1 January 2026) have formed a unified legal basis for the right to protect personal data.[68] This Decree stipulates seven foundational principles for processing data, including lawfulness, transparency, purpose limitation, and data minimisation. In particular, Articles 24 and 25 impose an obligation to conduct an impact assessment for high-risk data processing activities, laying the groundwork for a risk-prevention mechanism similar to the Data Protection Impact Assessment (DPIA) in EU Law.

The 2025 Law on Personal Data Protection expands the scope of protection, establishing the right of individuals to know, object, and request the termination of data processing, and clearly stipulates accountability for organisations, state agencies, and enterprises when processing data in judicial and administrative activities. However, the current Vietnamese legal framework still reveals some limitations as follows:

First, the regulations governing data processing in criminal justice activities remain fragmented, and a coordination mechanism among the Investigation Agency, the Procuracy, the Court, and the Data Management Agency has not yet been established. Meanwhile, the EU model clearly stipulates the role of independent Data Protection Authorities in supervising the processing of data for the purposes of investigation and prosecution.

Second, there are no specific regulations on accountability and risk assessment when applying AI in the justice sector. Current documents are mainly at the framework level and do not identify the agency responsible for appraising, approving, or supervising AI systems used in legal proceedings. This poses a potential risk of "automating judicial power," when the results generated by AI systems (for example: risk scoring, behavioural analysis) can directly influence investigation or adjudication decisions without being fully verified by humans.[69]

Third, the lack of an independent monitoring body for personal data protection–a "focal pillar" of the EU model. Currently, data management in Vietnam is dispersed between the Ministry of Public Security and the Ministry of Science and Technology, leading to overlapping responsibilities and a lack of a unified judicial and administrative monitoring mechanism.

Finally, the institutional and digital capacities of the judiciary team remain limited compared to practical requirements. The understanding and application of data protection principles, such as "necessary", "proportionate", and "human supervision",

[68] Decree of the Socialist Republic of Vietnam No 13/2023/ND-CP (n 8); Law of the Socialist Republic of Vietnam No 91/2025/QH15 (n 9).

[69] Mantelero (n 22; 23).

remain at the level of awareness and have not yet become mandatory standards in investigation and adjudication.

Therefore, although the initial legal foundation for ensuring the right to personal data protection has been established, the application of AI to criminal justice in Vietnam still requires integrated improvement, grounded in human rights and the control of high-risk technology. This involves a combination of institutional reform, the establishment of independent monitoring bodies, and capacity-building for legal proceedings and conducting bodies to achieve a dynamic balance between technological innovation and human rights protection. Recent developments provide important indications of rising risks and the urgent need for data protection mechanisms in the context of judicial digitalisation. In Ho Chi Minh City, a system of 31 AI-integrated cameras detected more than 3,100 violations within just over one month of operation, illustrating that behavioural data are being collected on a large and continuous scale.[70] On the other hand, the Ministry of Public Security dismantled a scheme involving the sale of nearly 56 million personal data records,[71] reflecting the severe vulnerability of individuals to data breaches. At the same time, the Ministry of Justice rose six places in the 2023 ministerial-level Digital Transformation Index.[72] It showed efforts to enhance the digital capacity of the justice sector—but also signalling the urgent need for corresponding risk-control mechanisms as technological applications continue to expand.

6.2. Challenges of Vietnam in Ensuring the Balance between Technological Innovation and the Right to Personal Data Protection in Criminal Justice

First, Vietnam currently lacks a specialised legal framework regulating the use of AI in criminal justice. The 2015 Criminal Procedure Code only recognises electronic data as a source of evidence (Articles 87 and 99). It does not regulate legal conditions, evidentiary value, or exclusion rules for data generated by AI systems. Litigation practice shows that there are challenges in authenticating, collecting evidence, and assessing the value of

[70] Vu Phuong, 'AI-Enabled Cameras Scanning the Streets of Ho Chi Minh City Detect More than 3,100 Traffic Violations' *Báo Thanh Niên* (Ho Chi Minh city, 5 October 2025) [in Vietnamese] <https://thanhnien.vn/camera-ai-quet-duong-pho-tphcm-phat-hien-hon-3100-truong-hop-vi-pham-giao-thong-185251005140705779.htm> accessed 21 November 2025.

[71] Hai Lan, 'A Trafficking Ring Trading Nearly 56 Million Personal Data Records Was Dismantled' *Báo Công An Nhân Dân* (Hanoi City, 21 February 2025) [in Vietnamese] <https://cand.com.vn/Ho-so-Interpol/triet-pha-duong-day-mua-ban-gan-56-trieu-du-lieu-ca-nhan-i759592/> accessed 21 November 2025.

[72] An Nhu, 'The Ministry of Justice Rose Six Places in the 2023 Digital Transformation Index' (*Bộ Tư pháp*, 6 February 2025) [in Vietnamese] <https://moj.gov.vn/qt/tintuc/Pages/hoat-dong-cua-lanh-dao-bo.aspx?ItemID=6810> accessed 21 November 2025.

electronic evidence, especially when AI technology is applied in activities of identifying, predicting, or analysing behaviour.[73]

Second, the DPIA mechanism is only stipulated at the principle-based level, without specific technical guidance on risk criteria, appraisal procedures, or approval agencies. Meanwhile, EU standards (Article 35 GDPR; EDPB Guidelines 4/2020) require that all high-risk data processing activities, especially in the justice and security fields, must undergo independent audits. The absence of this mechanism hinders Vietnam's ability to ensure a "dynamic balance" between technological innovation and human rights.

Third, the institutional capacity and human resources of the judiciary for auditing, explaining, and monitoring the operation of AI systems remain limited. Investigators, prosecutors, and judges are not fully equipped with the skills to understand, criticise, or verify the objectivity of algorithms. Meanwhile, studies by OHCHR[74] and the EU Agency for Fundamental Rights[75] have warned that the application of AI in law enforcement can lead to bias, discrimination, and privacy violations without human oversight and transparent accountability mechanisms.

Fourth, data sharing and interconnection between judicial agencies are limited and lack protection standards. Data is stored in a decentralised manner by each agency. There are no technical standards for anonymisation, encryption, or limitation of use. This not only affects the effectiveness of coordination in legal proceedings but also increases the risk of leakage or misuse.

Fifth, the standard for the right to personal data protection is not clearly defined in the Constitution. The 2013 Constitution (Article 21) only recognises the right to privacy and personal confidentiality, but does not recognise the right to personal data protection as an independent right. Meanwhile, international standards consider this right a "digital personality right" that helps regulate structural risks in the AI era. Without being constitutionalised, specialised laws lack a constitutional basis to establish an effective balancing mechanism between innovation and human rights protection.[76]

Overall, the above challenges show that Vietnam is only in the early stages of developing a "dynamic balance" model between technological innovation and the protection of personal

[73] Vo Minh Tuan, 'Difficulties and Barriers Regarding Electronic Data in the 2015 Criminal Procedure Code' [7 February 2021] Tạp chí Tòa án nhân dân điện tử [in Vietnamese] <https://tapchitoaan.vn/kho-khan-vuong-mac-ve-du-lieu-dien-tu-trong-bo-luat-to-tung-hinh-su-nam-2015> accessed 24 October 2025.

[74] OHCHR, 'The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights' (A/HRC/48/31, 13 September 2021) <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high> accessed 24 October 2025.

[75] FRA, *Facial Recognition Technology: Fundamental Rights Considerations in EU Law Enforcement* (Publications Office of the EU 2023).

[76] OHCHR (n 74); Council of Europe, *Convention 108+* (n 18).

data rights. To move towards a digital justice model that ensures human rights, Vietnam must shift from a reactive legal framework to a proactive one, in which all AI applications in criminal justice are grounded in lawfulness, necessity, proportionality, accountability, and human oversight. Moreover, reports from international organisations also indicate structural technological risks associated with the use of AI in judicial activities. The OHCHR report warns of algorithmic bias in facial recognition and crime-prediction systems, particularly in relation to women and minority groups.[77] Similarly, FRA reports high misidentification rates and the risk of biometric data leakage when law enforcement authorities store data on a large scale without adequate access controls.[78] These risks underscore the urgent need to design appropriate oversight and impact-assessment mechanisms as Vietnam expands the use of AI in criminal justice.

Compared with the EU, Vietnam shares the same core values of personal data protection but differs in institutionalisation and enforcement. The EU mandates Data Protection and Fundamental Rights Impact Assessments (DPIA/FRIA) and empowers independent supervisory authorities, while Vietnam only outlines general principles and distributes authority across multiple agencies. This gap reflects not only differences in capacity but also the need for selective and context-appropriate legal adaptation.

7 RECOMMENDATIONS TO IMPROVE VIETNAM'S LEGAL SYSTEM FROM THE EUROPEAN UNION'S EXPERIENCE

Based on the EU's experience, this section proposes directions for improving the law and policy implications to help Vietnam ensure a "dynamic balance" between technological efficiency and human rights. However, it is necessary to understand that strengthening personal data protection in criminal justice is a long-term undertaking that requires continuous and incremental institutional adjustment. As a developing country, Vietnam must simultaneously undertake many other important strategic tasks, particularly economic development; therefore, legal reforms in this area need to be implemented through a multi-stage roadmap, prioritising the improvement of the legal framework and enforcement capacity, and only subsequently moving toward independent oversight mechanisms and adequate technological infrastructure.

(1) *Leverage the right to personal data protection to constitutional standards.* Vietnam's 2013 Constitution addresses this right only in Article 21 on privacy and correspondence. Elevating it to a constitutional or statutory level would (i) reinforce the rule of law in the digital era by subjecting technological activities in justice to constitutional oversight, and (ii) provide a legal basis for balancing rights with public interests and crime prevention. As a first step, this could be detailed in the 2025 Law

[77] OHCHR (n 74).

[78] FRA (n 75).

on Personal Data Protection's guiding documents, paving the way for future constitutional reform.

(2) *Complete the Criminal Procedure Code on "digital evidence detected or found with the support of AI"*. Currently, the 2015 Criminal Procedure Code only stipulates electronic data as a type of evidence (Article 99) without any legal standards for evidence detected or found with the support of AI. Therefore, it is essential to add a specialised sub-section on AI evidence to the Criminal Procedure Code, including: conditions of acceptance (model transparency, explainability, and independent verification); exclusion rules for evidence violating the right to personal data protection; the obligation to keep technical traces (traceability); and the right to challenge the algorithm of the defender.

(3) *Add a data impact assessment mechanism (DPIA/FRIA).* Vietnam could adopt an EU-style mechanism requiring mandatory DPIAs for all AI projects in investigation, adjudication, and enforcement, with both ex-ante and ex-post reviews by a data oversight body. In the short term, this could be specified in the Decree guiding the 2025 Law on Personal Data Protection, incorporating a verification process akin to "professional approval" in healthcare. Vietnam should also establish an independent National Data Protection Authority, empowered to supervise data handling in criminal proceedings in coordination with the Supreme People's Procuracy—similar to the EU's EDPB—to enhance transparency and public trust in judicial digitalisation.

(4) *Establish a separate legal framework for AI in the criminal justice system.* Vietnam could develop a principles-based legal framework for judicial AI covering three areas: (i) defining judicial AI, (ii) classifying risks and corresponding liabilities, and (iii) creating a regulatory sandbox for technologies in adjudication and enforcement. This could be piloted at the Supreme People's Court and the Ministry of Public Security, following the State Bank's fintech sandbox model. At the same time, a national human rights–oriented AI policy for criminal justice that defines the scope of AI use across investigation, prosecution, adjudication, and enforcement, and establishes ethical, technical, and legal safeguards. Vietnam may adopt the EU's "Human Rights Impact Assessment" model to evaluate and disclose data-sensitive technologies. This is feasible given the foundations established under Decree No. 13/2023/NĐ-CP and the 2025 Law on Personal Data Protection, which already require DPIAs.

(5) *Refine the policy of training, fostering digital capacity, and technology ethics for judicial staff.* Vietnam should establish a continuous training program on "judicial data governance" and, through international cooperation within the EU-ASEAN or UNESCO frameworks, exchange experiences and methods for technology verification. The investment in human capacity will determine the level of success of the process of "humanising digital justice".

(6) *The State can encourage technology enterprises to participate in research, testing, and the development of judicial support tools,* such as electronic record management systems, digital evidence analysis, or virtual assistants for conducting legal proceedings. But these tools must be subject to independent verification of data risks and human rights impacts. This approach encourages innovation and ensures that the private sector cannot dominate or undermine the independence of the judicial activities.

(7) *Promote international cooperation on judicial technology.* Vietnam should participate in international initiatives, such as the Global Partnership on AI (GPAI) or the OECD.AI Policy Observatory program. This can support Vietnam in approaching global standards on responsible AI and personal data protection. Additionally, it is necessary to promote bilateral judicial dialogue with the EU within the framework of implementing the EVFTA and EVIPA, to learn about mechanisms to ensure data rights in the cross-border judicial environment.

The above analysis shows that the EU has achieved balance through three institutional pillars: the constitutional right to data protection, mandatory impact assessments, and independent lifecycle supervision. Vietnam is gradually approaching this model through the 2025 Law on Personal Data Protection and the revision of the Criminal Procedure Code. Incorporating these elements domestically will promote "responsible innovation," a crucial step toward safeguarding human rights in the digital justice system.

8 CONCLUSIONS

The rapid development of AI is reshaping criminal justice, especially in evidence collection, processing, and evaluation. Along with the obvious benefits in efficiency, speed, and analytical capabilities, this technology also poses challenges for human rights protection, with the right to data protection becoming a focus of contemporary legal debate.

The experience of the EU shows that "balancing" between technological innovation and human rights protection is not a choice between two opposite poles, but a continuous process of legal governance. The EU has built a systemic regulatory model – combining a constitutional basis for the right to personal data, risk assessment and accountability mechanisms, risk–based management, and independent monitoring and judicial control. For Vietnam, the promulgation of the 2025 Law on Personal Data Protection and the adoption of digital transformation policies in criminal justice mark an essential step forward. However, to achieve a sustainable balance between technological innovation and the protection of human rights, it is necessary to establish a comprehensive legal framework that clearly sets out the scope, limits, and control mechanisms for the use of AI in criminal proceedings.

REFERENCES

1. An N, 'The Ministry of Justice Rose Six Places in the 2023 Digital Transformation Index' (*Bộ Tư pháp*, 6 February 2025) [in Vietnamese] <https://moj.gov.vn/qt/tintuc/Pages/hoat-dong-cua-lanh-dao-bo.aspx?ItemID=681> accessed 21 November 2025
2. Daly A and others, 'Artificial Intelligence, Governance and Ethics: Global Perspectives' (Research Paper no 2019-15, The Chinese University of Hong Kong Faculty of Law 2019) doi:10.2139/ssrn.3414805
3. Hai L, 'A Trafficking Ring Trading Nearly 56 Million Personal Data Records Was Dismantled' *Báo Công An Nhân Dân* (Hanoi City, 21 February 2025) [in Vietnamese] <https://cand.com.vn/Ho-so-Interpol/triet-pha-duong-day-mua-ban-gan-56-trieu-du-lieu-ca-nhan-i759592/> accessed 21 November 2025
4. Mantelero A, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) Computer Law & Security Review 754. doi:10.1016/j.clsr.2018.05.017
5. Mantelero A, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020. doi:10.1016/j.clsr.2024.106020
6. Milaj J, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2016) 30(3) International Review of Law, Computers & Technology 115. doi:10.1080/13600869.2015.1076993
7. Stahl BC and others, 'Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning' (2021) 124 Journal of Business Research 374. doi:10.1016/j.jbusres.2020.11.030
8. Trykhlib K, 'The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights' (2020) 4 EU and Comparative Law Issues and Challenges Series (ECLIC) 128. doi:10.25234/eclic/11899
9. Vo MT, 'Difficulties and Barriers Regarding Electronic Data in the 2015 Criminal Procedure Code' [7 February 2021] Tạp chí Tòa án nhân dân điện tử [in Vietnamese] <https://tapchitoaan.vn/kho-khan-vuong-mac-ve-du-lieu-dien-tu-trong-bo-luat-to-tung-hinh-su-nam-2015> accessed 24 October 2025
10. Vu P, 'AI-Enabled Cameras Scanning the Streets of Ho Chi Minh City Detect More than 3,100 Traffic Violations' *Báo Thanh Niên* (Ho Chi Minh city, 5 October 2025) [in Vietnamese] <https://thanhnien.vn/camera-ai-quet-duong-pho-tphcm-phat-hien-hon-3100-truong-hop-vi-pham-giao-thong-185251005140705779.htm> accessed 21 November 2025
11. Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review 494

AUTHORS INFORMATION

Phuong Anh Nguyen
Master of Law, PhD candidate, Faculty of Criminal Law, Hanoi Law University, Hanoi, Vietnam
phuonganhlawb@gmail.com
https://orcid.org/0009-0002-3555-3003
Corresponding author, solely responsible for the manuscript preparing.

Competing interests: No competing interests were disclosed.

Disclaimer: The author declares that their opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

Managing Editor – Mag. Yuliia Hartman. **English Editor** – Julie Bold.
Ukrainian language Editor – Mag. Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article
Nguyen PA, 'Artificial Intelligence in Criminal Justice: Balancing Technological Innovation and Personal Data Protection Rights. A Comparative Legal Study between the European Union and Vietnam' (2025) 8(Spec) Access to Justice in Eastern Europe 233-58 <https://doi.org/10.33327/AJEE-18-8.S-r000161>

DOI: https://doi.org/10.33327/AJEE-18-8.S-r000161

Summary: 1. Introduction. – 2. Methodology. – 3. Concept Framework. – *3.1. The Definition of "Artificial Intelligence in Criminal Justice"*. – *3.2. The Definition of "Technological Innovation in Criminal Justice"*. – *3.3. The Definition of "Right to Personal Data Protection in Criminal Justice"*. – 4. Key Principles Ensuring a Balance between Technological Innovation and the Right to Personal Data Protection. – *4.1. The Principles of Lawfulness, Necessity, and*

Proportionality. – 4.2. The Principle of Accountability and Impact Assessment. – 4.3. The Principle of Transparency and Human Supervision. – 4.4. The Principle of a Balanced Approach in Applying AI to Criminal Justice. – 5. The EU's Experience in Ensuring the Balance between Technological Innovation and Personal Data Protection in Criminal Justice. – *5.1. The EU's Legal Framework for Ensuring the Balance between Technological Innovation and Personal Data Protection. – 5.2. Balancing Mechanisms through Impact Assessment and Risk Control. – 5.3. Enforcement Mechanism and the Role of Independent Monitoring Bodies.* – 6. Legal Status and Challenges in Vietnam in Ensuring a Balance between Technological Innovation and Personal Data Protection in Criminal Justice. – *6.1. Current Status of Vietnamese Laws. – 6.2. Challenges of Vietnam in Ensuring the Balance between Technological Innovation and the Right to Personal Data Protection in Criminal Justice.* – 7. Recommendations to Improve Vietnam's Legal System from the European Union's Experience. – 8. Conclusions.

Keywords: *artificial intelligence, criminal justice, right to personal data, human rights, European Union, Vietnam.*

DETAILS FOR PUBLICATION

Date of submission: 26 Oct 2025
Date of acceptance: 08 Dec 2025
Online First publication: 19 Dec 2025
Last Published: 30 Dec 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 3 reports
Number of revision rounds: 1 round with minor revisions

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The author confirms that AI technologies have only been used to enhance language clarity and grammar. No AI tools were used to generate ideas, structure arguments, analyze data, or produce conclusions.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНОМУ СУДОЧИНСТВІ: БАЛАНС МІЖ ТЕХНОЛОГІЧНИМИ ІННОВАЦІЯМИ ТА ПРАВОМ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ. ПОРІВНЯЛЬНО-ПРАВОВЕ ДОСЛІДЖЕННЯ ПІДХОДІВ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА В'ЄТНАМУ

Фуонг Ан Нгуєн

АНОТАЦІЯ

Вступ. *Швидкий розвиток штучного інтелекту сильно змінив різні аспекти суспільного життя, зокрема систему кримінального судочинства. У кримінальному провадженні збір та обробка біометричних, поведінкових та емоційних даних може загрожувати праву на приватність, презумпції невинуватості та праву на справедливий суд. У цьому дослідженні розглядається взаємозв'язок між технологічними інноваціями та захистом персональних даних у кримінальному судочинстві Європейського Союзу та В'єтнаму. За допомогою порівняльно-правового аналізу Загального регламенту про захист даних (GDPR) ЄС, Директиви про правоохоронну діяльність та Акту ЄС про ШІ 2024 року разом із правовою базою В'єтнаму, у статті визначено ключові сфери конвергенції, розбіжностей та регуляторних прогалин.*

Методи. *У дослідженні використовується порівняльно-правовий аналіз у поєднанні з підходом, що ґрунтується на правах людини, для уточнення взаємозв'язку між технологічними інноваціями та правом на захист персональних даних у кримінальному судочинстві. Джерелами інформації є правові бази Європейського Союзу та В'єтнаму, судова практика та звіти органів ЄС та Організації Об'єднаних Націй.*

Результати та висновки. *Метою дослідження є встановлення фундаментальних правових принципів, які забезпечують баланс між технологічними інноваціями та захистом права на персональні дані у кримінальному судочинстві — підхід, якому приділяється недостатня увага у В'єтнамі. На основі цього було запропоновано правові реформи, спрямовані на створення системи «цифрового правосуддя, орієнтованого на права людини», яка гарантуватиме, що цифровізація та застосування штучного інтелекту в системі правосуддя не лише підвищать операційну ефективність, але й зможуть зміцнити верховенство права та захистити людей.*

Ключові слова: *штучний інтелект, кримінальне судочинство, право на захист персональних даних, права людини, Європейський Союз, В'єтнам.*