THE IMPACT OF TECHNOLOGICAL DEVELOPMENTS ON HUMAN RIGHTS: LESSONS FROM THE EUROPEAN UNION AND RECOMMENDATIONS FOR VIETNAM

Pham Thi Minh Trang
Lecturer, Commercial Department, Ho Chi Minh City University of Law (Vietnam)
Doctorate Student, Doctoral School of Law, University of Pécs (Hungary)
Corresponding address: ptmtrang@hcmulaw.edu.vn
ORCID: 0009-0002-2291-2724

DOI: 10.47272/KIKPhD.2025.3.3

ABSTRACT
The development of technology is acknowledged as a great achievement of human beings. It facilitates connection and globalization, but also supports socio-economic development. Technology, particularly the existence of Artificial Intelligence, enhances convenience in daily life and promotes more efficient methods of working and conducting business. However, rapid technological growth may cause the legal framework to fall behind and pose challenges to the fundamental rights and values of human beings. This paper examines Vietnam's current legal framework for human rights protection, as well as its practice of implementation. It also analyzes the General Data Protection Regulation, the Artificial Intelligence Act, and other relevant European Union documents to gain experience from the European Union. Then, this paper will propose some recommendations to address gaps in Vietnamese regulations and strengthen the protection of human rights.

KEYWORDS
Personal data; biometric identifier; freedom of expression; technological development; non-discrimination.

ARTICLE HISTORY
SUBMITTED 19 Dec 2025 | REVISED 21 Dec 2025 | ACCEPTED 28 Dec 2025

I. Introduction

The technologies are rapidly developing and significantly impacting all sectors of socio-economic, as well as human rights. In Vietnam, the internet was introduced officially in 1997. With its sharp development, it has become a core infrastructure for the country's digital transformation.[1] As of January 2024, Vietnam had 78.44 million internet users, accounting for 79.1% of the population, with an average daily usage time of nearly seven hours.[2] Additionally, social media platforms have experienced steady growth since 2008. They have created a vast network that connects to the lives and work of most people. In particular, the rapid and explosive development of AI has marked a turning point that drives economic and social progress. Technical developments have facilitated a comfortable and convenient life for human beings, especially with the advent of the Internet, social media platforms, Artificial Intelligence (AI), and Big Data.

However, while the technological developments bring a variety of advantages, they also pose high risks of violating human rights. In Vietnam, personal data leaks are becoming increasingly frequent and complex. According to the 2024 Survey of the National Cybersecurity Association, there are 73.99% of users consider their data leaks occur because they provide personal information when shopping online, and 62.13% attribute the leaks to sharing information on social media.[3] As a result, fraud has become increasingly prevalent, particularly through phone calls and bank account hacking. Meanwhile, personal data, particularly biometric identifiers, is integrated into most personal devices and application accounts. If cybercrimes or hacker attacks occupy this data, the damage is unimaginable.

On the other hand, cyberspace has gradually evolved into an online environment where people can connect and share with one another worldwide. Therefore, establishing legal rules to safeguard the right to freedom of expression on cyberspace has become a prerequisite and an urgent obligation in the digital era. These rules help prevent violations of privacy and protect the legitimate interests of individuals and organizations, while also creating favourable conditions for building a democratic society. Moreover, while AI offers significant benefits for the socio-economic aspects, it also poses high risks to the protection of human rights.

[1] Tran Xuan Tien, 'Artificial Intelligence: Challenges to the Legal Profession in the New Era' (2024) Vietnam Lawyer Journal https://lsvn.vn/cong-nghe-ai-thach-thuc-doi-voi-nghe-luat-trong-thoi-dai-moi-a149640.html accessed 12 October 2025

[2] 'Vietnam's Internet: Thirty Years of Remarkable Growth' (*Ministry of Science and Technology*, 27 December 2024) https://mst.gov.vn/internet-viet-nam-ba-muoi-nam-phat-trien-than-toc-19724122712285863 8.htm accessed 14 October 2025

[3] Duy Anh, 'In 2024, the personal data of more than 66% of Internet users was used without authorization' (*Vietnam Lawyer Journal*, 2024) https://lsvn.vn/du-lieu-ca-nhan-cua-hon-66-nguoi-dung-internet-bi-su-dung-trai-phep-trong-nam-2024-a151492.html accessed 14 October 2025

Especially, AI discrimination has occurred when some AI systems produce biased output data or make unfair decisions, which negatively affect individuals and groups of people.

Therefore, this paper will focus on addressing three key issues, including: the right to personal data protection, the right to freedom of expression in Cyberspace, and Artificial Intelligence and the fight against Discrimination. This paper analyzes and evaluates the current regulatory framework in Vietnam and examines relevant EU regulations to draw lessons from the EU's experience. It then clarifies the challenges to protecting human rights that arise in the context of legal implementation during an era of rapid technological developments. This paper also provides some recommendations to strengthen the protection level of human rights in Vietnam's legal framework.

II. The Right to Personal Data Protection

1. Personal Data and Current Practices in Viet Nam

In the technology era, where technology has become an integral part of our daily lives,[4] people increasingly use and interact on digital platforms. It gives rise to the storage and sharing of personal data in a digital environment. In Vietnam, several websites for online shopping, e-marketplaces (such as Shopee, Tiki, TikTok Shop, and Lazada), social media platforms, and applications related to transportation, food services, or other utilities collect and store a huge amount of personal data. Moreover, in the process of building a digital society, the Ministry of Justice affirmed that personal data of more than two-thirds of the population is being posted, collected, stored, and shared online in various forms and at different levels of detail.[5] In the meantime, personal data has become a valuable resource for economic activities with high commercial value in this period.

'Personal data' means any information relating to an identified or identifiable natural person. According to the General Data Protection Regulation (GDPR)[6], it may include information that directly or indirectly identifies a natural person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1)). Under

[4] Vlona Pollozhani Shehu and Visar Shehu, 'Human rights in the technology era – Protection of data rights' (2023) 7(2) European Journal of Economics, Law and Social Sciences 1. https://doi.org/10.2478/ejels-2023-0001

[5] Ministry of Justice of Viet Nam, 'The Proposal to Develop the Law on Personal Data Protection' (2024) https://datafiles.chinhphu.vn/cpp/files/duthaovbpl/2024/Thang09/1.totrinhluatbaovedulieucanhan.doc accessed 10 January 2026

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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)

Vietnamese regulations, personal data is divided into two types: basic personal data and sensitive personal data. According to Article 2(2) of the Law on Personal Data Protection 2025, 'Basic personal data'[7] refers to personal data reflecting common personal details and background information, frequently used in transactions and social relations. Article 2(3) of this Law also provides a definition of 'Sensitive personal data'[8]. It refers to personal data associated with individuals' privacy rights that, if infringed on, directly affect the legitimate rights and benefits of agencies and organizations.

Notably, among these types of personal data, biometric data is a form of sensitive data that is increasingly used in the technological development era, providing several effective solutions in various areas, particularly in identification methods. The right to identity is a fundamental right, recognized by Article 6 of the Universal Declaration of Human Rights (UDHR): *"Everyone has the right to recognition everywhere as a person before the law"*. Accordingly, each country has its own mechanisms for identifying its citizens. In traditional methods, the identification of a person can be recognized by a classical photograph on a passport or ID card. However, with advances in technology, biometric identifiers have become new methods that are gradually replacing these older forms of identification due to their convenience, sophistication, and high level of accuracy. Biometric technologies describe the range of tools and procedures used to analyse, measure and record one or more of these unique human characteristics.[9] They collect and generate biometric data, which includes unique physical and biometric characteristics of an individual to identify them. These data are increasingly sophisticated and measurable parameters.

In the legal sector and management of the State, the 2023 Law Identification provides a definition of "biometric identifiers"[10]. There are some popular types of biometric identifiers, including fingerprint, facial scan, voice

[7] Basic personal data was specified by the Government by giving a list of basic personal data. It may include: a name, date of birth, date of death or disappearance, gender, place of birth, place of residence, contact address, nationality, personal image, phone number, personal identification number, passport number, driver's license number, marital status, information on family relationships, information on a person's digital accounts, etc. (Article 3 of Decree 365/2025/ND-CP Detailed Regulations on the Implementation of Certain Articles and Measures for the Enforcement of the Law on Personal Data Protection)

[8] Sensitive personal data includes information revealing racial or ethnic origin, political or religious beliefs, private or family life, health status, biometric or genetic data, sexual life or orientation, criminal records, location data, login credentials and identification documents, financial or banking information, etc. (Article 4 of Decree 365/2025/ND-CP)

[9] Robert Brumnik and Iztok Podbregar, 'Biometric Technology and Human Rights' (2010) 7 (1) US-China Law Review 1.

[10] Article 3(3) of the 2023 Law Identification, "*Biometric identifiers"* mean biometric or biological characteristics that are distinctive and stable of a person, used to identify and distinguish such person from another one

recognition, iris recognition, and DNA[11]. These serve as effective tools and are suitable for a wide range of purposes. Vietnamese citizens from the age of 14 must carry out procedures for the issuance of an ID card.[12] As a result, the authorities will collect personal information such as name, address, date of birth, gender, and biometric identifiers as specified in Article 18 of this Law. Thus, citizens have the obligation to provide personal information and biometric identifiers, except for DNA and voice[13]. Personal data is collected and stored in the identification database, which can be extracted by State agencies, political organizations, and socio-political organizations, depending on performing their functions and tasks. The extraction of information from the database is strictly regulated, as it requires the consent of both the competent authority and the individuals whose personal data are involved.

At the same time, in the banking sector, beyond basic personal data, biometric technologies have been widely applied in recent years. Under Circular No 17/2024/TT-NHNN on Opening and Use of Checking Account at Payment Service Provider (came into force from July 1, 2024), biometric information of account holders, in the case of individual customers, or of legal representatives, in the case of organizational customers, must be collected when checking accounts are opened electronically at banks and foreign bank branches. With customers who already have accounts, cash withdrawal and e-transactions made via checking accounts are only allowed when personal identification documents and biometric information are cross-checked. Therefore, e-wallets or integrated payment accounts on e-marketplaces or websites must undergo biometric verification to continue to be used.

In the above situations, personal data is compulsorily collected in accordance with legal regulations; however, in practice, it is also collected and used by numerous other actors for various purposes and at different levels. It is evident that there is an imbalance in the way information technology is used. Many people have a mindset that they are willing to trade personal and private information for technological convenience. Besides, during the training and utility of AI, people also provided a lot of important personal information. Therefore, a segment of the population is ready to disclose personal information on digital platforms without full consideration of the potential risks. In other words, the awareness of most Vietnamese users regarding personal data protection remains relatively low. Meanwhile, the potential for data leaks on these online platforms and applications is significantly high because existing security measures are inadequate, and measures to combat data abuse are also not clearly defined. With the vast scope and diverse

[11] Article 15 of the 2023 Law Identification No 26/2023/QH15 dated November 27, 2023

[12] Article 19 of the 2023 Law Identification

[13] Because both are voluntarily provided by each citizen or collected by the criminal proceedings agency or the supervisory agency of persons against whom administrative measures are taken

levels of data collection in cyberspace while cybercrimes, online fraudulent schemes, and deepfake identity fraud have become increasingly sophisticated.

2. Regulations on the protection of personal data

Regarding regulations on the protection of personal data, from an international perspective, the GDPR is one of the pioneering instruments regulating the protection of personal data and biometric data; however, this legal field is still relatively new in Vietnam. The first legal instrument that directly regulated the protection of personal data was promulgated by the Government in 2023, Decree No. 13/2023/ND-CP on the Protection of Personal Data. This Decree provides a fundamental legal basis for protecting personal data amid the rapid development and application of biometric technologies. It sets out a legal basis for enhancing the management of the collection, processing, and transfer of personal data, as well as mitigating risks during this period. Although this Decree draws on many experiences of the GDPR, differences in legal systems, economic conditions, social factors, existing precedents on personal data protection[14], and limited legislative experience in this field have resulted in several limitations in the initial Decree.

During this period, many companies, particularly service businesses, collect customers' personal data and allow third-party partners to access such data with lax requirements or safeguards. As a result, third parties can transfer or trade personal data to other entities. The purchasing and selling of personal data has become increasingly complex through numerous sophisticated methods. However, the violations have not been specified, which impairs the effectiveness of law enforcement. Civil, administrative, and criminal sanctions are either insufficiently deterrent or, in some cases, have not yet been established.

Therefore, on June 26, 2025, the legislative body (the National Assembly) further developed and refined numerous new elements for the promulgation of the first Law on Personal Data Protection. This law took effect on January 1, 2026, replacing Decree 13/2023/ND-CP, and aims to strengthen the level of protection of personal data. It is a foundational legal instrument at the statutory level on the protection of personal data in general, as well as biometric data in particular. Moreover, this Law is further detailed in Decree No. 356/2025/ND-CP, which also took effect on the same date. It provides detailed regulations on the implementation of certain Articles and measures for the enforcement of the Law on Personal Data Protection.

[14] Ministry of Justice of Viet Nam, the Proposal to Develop the Law on Personal Data Protection (2024) https://datafiles.chinhphu.vn/cpp/files/duthaovbpl/2024/Thang09/1.totrinhluatbaovedulieucanhan.doc accessed 10 January 2026

According to this Law, the legal framework for protecting personal data is strengthened more than in the previous Decree. It can be proved by the following points:

First, previously, the protection of personal data was recognized primarily as a set of rights, but it lacked effective enforcement mechanisms. However, the Law on Personal Data Protection establishes detailed regulations, such as the methods, duration, and necessary procedures to give effect to the protection of human rights. For example, the consent and withdrawal of consent of the data subject are set out in Articles 9, 10, and 19 of this Law. Accordingly, to process personal data, the data subject has to give consent in a clear and specific manner,[15] except for the processing of some cases, such as to protect the life, health, and legitimate rights of the personal data subject; to respond to emergencies to national security; to serve the state management according to the law, etc. Besides, this law lays down the conditions for withdrawal of consent, the legal mechanisms, as well as the responsibility of the controlling party.

Moreover, the Law also supplements the detailed regulations on the handling of violations of personal data protection. In other words, as a result of the GDPR experience, the Law establishes stricter sanctions for such violations. Depending on the nature, severity, and consequences of the violation, organizations or individuals may be subject to civil, administrative, or criminal liability. Notably, illegal trading in personal data and unlawful cross-border transfers of personal data may be subject to administrative fines amounting to a significant proportion of revenue, including fines of up to 10 times the revenue obtained from the violation or up to 5% of total revenue, respectively.

Secondly, the provision on notices of violations against personal data protection regulations is regulated for the first time, aiming to promptly detect and remedy violations (Article 23 of the Law on Personal Data Protection). Specifically, when the data controller, the data processor, or a third party detects violations of personal data protection regulations that may harm national defence, security, social order, or public safety, or infringe upon the life, health, honour, dignity, or property of the personal data subject, they shall notify the personal data protection authority within 72 hours of detecting such violations. They shall also promptly inform relevant parties to prevent or mitigate damage.

In addition, agencies, organizations, and individuals may actively participate in protecting personal data. Where they detect personal data being

[15] Methods for obtaining the consent of data subjects shall ensure verifiability, including the ability to identify that consent has been given by the data subject, as well as the time and content of such consent. Consent may be obtained in writing; through recorded telephone calls; via consent messages sent by mobile text message; through email, websites, platforms, or applications equipped with technical mechanisms for obtaining consent; or by other appropriate methods that can be printed or reproduced in written form, including electronic documents or other verifiable formats. (Decree No. 356/2025/ND-CP).

processed for improper purposes or in violation of agreed terms, or where the rights of data subjects are not ensured, they may report such violations to the competent authorities. Moreover, the responsibilities of these entities are governed by this Law. Enhanced cooperation among these entities, with clearly defined deadlines, can promote voluntary compliance of relevant subjects.

Thirdly, the Law also supplements specific regulations governing foundation sectors, as well as emerging fields. For example, regarding social media platforms and online communication services, they have rapidly expanded their user bases and have become potential sources of personal data leakage. According to Article 29 of the Law on Personal Data Protection, providers of social media and online communication services are required to offer a "Do Not Track" option or to track user activities only with the data subject's consent. Furthermore, eavesdropping, wiretapping, recording calls, or reading text messages without the consent of the personal data subject is strictly prohibited. Notably, service providers are not permitted to request images or videos containing all or part of personal identification documents for account verification purposes. Besides, confidentiality policies and the methods of collecting, using, and sharing personal data must be clearly disclosed and explained to users.

On the other hand, Article 31 of this Law sets out strict standards for the protection of personal location data and biometric data. In particular, it clarifies the prohibition of unlawful location tracking and defines the obligations of mobile application platform providers when collecting or using personal location data. Regarding biometric data, the collection and processing have to enhance the adoption of physical confidentiality measures for their biometric data transmission and storage devices; restrict rights to access to biometric data, and establish monitoring systems to prevent and detect acts of infringement.

Furthermore, personal data in environments such as big data, artificial intelligence (AI), blockchain, virtual spaces, and cloud computing is regulated to provide guidance on data processing, clarify risk levels for the application of appropriate personal data protection measures, and ensure compliance with ethical standards and Vietnamese customs (Article 30).

In short, the Law on Personal Data Protection lays down the rights of personal data subjects and the obligations of controllers and processors, and revises the sanctions applicable to violations of personal data protection rules. Although the rights provided under Vietnamese Law remain more limited than those under the GDPR, this Law represents a significant step forward. For example, the Law does not recognize the right to data portability, which under the GDPR allows data subjects to receive their personal data and transmit it directly from one controller

to another.[16] However, it cannot be denied that Vietnamese Law has drawn lessons from the GDPR and has been considerably improved compared to Decree No. 13/2023/ND-CP, such as data protection impact assessments (Articles 21 and 22 of the Law) and the obligation to notify personal data breaches to the supervisory authority (Article 23). Therefore, the effective implementation of this Law, together with the strengthening of human rights protection, requires a clear roadmap for further development and refinement. This journey also needs to take into account Vietnam's socio-economic conditions in order to progressively raise the level of personal data protection.

III. The Right to Freedom of Expression in Cyberspace

One of the equally important issues in the protection of human rights during the technology era is cybersecurity and the right to freedom of expression. On the one hand, freedom of expression is a fundamental right of every human being. This right constitutes essential foundations for democracy, rule of law, peace, stability, sustainable, inclusive development and participation in public affairs.[17] Under Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Alongside the exercise of this right, individuals must also fulfill certain duties and responsibilities to ensure the interests of the State and other persons. These obligations serve the interests of national security, territorial integrity, and public safety; the prevention of disorder or crime; the protection of health or morals; the safeguarding of the reputation or rights of others; the prevention of the disclosure of confidential information; and the preservation of the authority and impartiality of the judiciary.

On the other hand, cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[18] In cyberspace, a communication system and information processing are created where people's activities are not limited by space and time. In other words, cyberspace or the Internet is where shared information and social interactions occur, and it has

[16] Andreas Nicolas Häuselmann, 'EU privacy and data protection law applied to AI: Unveiling the legal problems for individuals', Doctoral thesis, Universiteit Leiden (2024) https://core.ac.uk/download/612047553.pdf accessed 21 January 2026

[17] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

[18] U. M. Mbanaso and E.S. Dandaura, 'The Cyberspace: Redefining A New World' (2015) 17(3) IOSR Journal of Computer Engineering 18. https://doi.org/10.9790/0661-17361724

become a central part of modern life.[19] It has transformed various aspects of society, including commerce, entertainment, and communication.[20] In early 2025, Vietnam had 79.8 million internet users, with 78.8% of the population connected online.[21] According to the 2024 Report of the Ministry of Information and Communications, there are approximately 110 million Vietnamese people using social networks. Zalo records 76.5 million monthly active users, Facebook has 72 million users, and TikTok reaches 67 million users, etc.[22] Moreover, the Government and relevant authorities have official websites and social media accounts with large followings. It plays an effective disseminating information and conducting public communication.

However, the more development and expansion of cyberspace, the greater the risk it is to cyber-attacks, thereby posing greater risks to users and information systems. Threats to cybersecurity can include computer viruses, spam, identity theft, data breaches, denial of service attacks, and cybercrime.[23] The EU and some other countries have declared the issue of cybersecurity, and specifically cyber attacks against their governments and citizens, as a national security threat and have developed national cybersecurity strategies or initiatives.[24]

Moreover, sharing of personal information, daily activities, thoughts, feelings, or status updates has become common, even gradually replacing traditional communication methods. Because digital platforms involve a wide range and are difficult to control, individuals may intentionally or unintentionally disclose sensitive information. In certain cases, such platforms can be misused as tools to act against the State or to disseminate content that harms, insults, or defames other individuals or organizations. The abuse of freedom of expression, especially on social networks to spread misinformation and cause public confusion, has become increasingly common. In many cases, such acts aim to undermine the government or attack other entities. Given the speed at which information spreads and the powerful influence

[19] Kafi Mahmud, Ehashan Ahmed, Zaedul Islam, Baki Billah, Biplob Banarjee, KariulIslam, 'Freedom of Expression in Cyberspace: Society, Law and its Effects in Bangladesh's Perspective' (2024) 44(4) Library Progress International 843.

[20] Ibid. 844.

[21] DataReportal, Vietnam Digital Overview Report 2025 https://cleverads.vn/blog/digital/ accessed 5 November 2025

[22] Minh Sơn, 'Which social media platform is the most widely used in Vietnam?' (*Ministry of Science and Technology*, 29 December 2024) https://mst.gov.vn/mang-xa-hoi-nao-duoc-nhieu-nguoi-dung-nhat-tai-viet-nam-19725010716061544 6.htm accessed 2 November 2025

[23] Carolina Rossini And Natalie Green, 'Cybersecurity and Human Rights' (*gp-digital*, 2015) https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf accessed November 15, 2025

[24] Minh Sơn, 'Which social media platform is the most widely used in Vietnam?' (*Ministry of Science and Technology*, 29 December 2024) https://mst.gov.vn/mang-xa-hoi-nao-duoc-nhieu-nguoi-dung-nhat-tai-viet-nam-19725010716061544 6.htm accessed 2 November 2025

of social media, this can cause significant harm, including damage to reputation, dignity, and public trust.

Therefore, it is an essential factor in ensuring a safe digital environment and mitigating potential threats. This is a precondition for the implementation of the right to freedom of expression, as well as ensuring social security. Drawing on the EU's experience, the EU will pay particular attention to key issues to promote and protect the right to freedom of expression.

One of these is combating violence, persecution, harassment, and intimidation of individuals, including journalists and other media actors.[25] Under a judgment of the European Court, a higher level of protection for journalistic reporting on matters of public interest, also recognising "the right of the public to be properly informed" about matters of interest for society.[26] Accordingly, any actions that infringe upon or threaten individuals for exercising their right to freedom of expression must be publicly condemned. The EU calls on all Member States to prevent violence against journalists and other media actors, and to promote the exchange of awareness-raising initiatives and training measures aimed at preventing attacks.

Besides, enhance programmes for exchanging opinions and expressions with all relevant stakeholders, such as law enforcement officers, the judiciary, civil society, politicians, human rights defenders, lawyers, security forces, academics, and religious or cultural agencies[27], to strengthen the protection and promotion of the right to freedom of expression. Member States research and improve the Law, aiming to limit excessive interference by authorities in the exercise of the right to freedom of expression when such expression does not infringe upon the rights of others. The authorities encourage whistleblowers to report abuse of these rights to violate the interests or privacy of individuals, organizations. On the other hand, requirements for creating and verifying social media accounts serve as an effective tool to reduce risks and help build a safer online environment where individuals can exercise their right to freedom of expression. Alongside this, strong account

[25] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

[26] Dirk Voorhoof, 'The Right to Freedom of Expression and Information under the European Human Rights System: Towards a more Transparent Democratic Society' (Working Papers of RSCAS 2014/12 Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom) https://cadmus.eui.eu/server/api/core/bitstreams/c6386959-9781-5723-a94c-932056331aeb/content accessed 10 November 2025

Balázs Hohmann, 'Integrity Advisors and the Development of Administrative Communication Culture' (2019) 4(1) European Journal of Multidisciplinary Studies https://doi.org/10.26417/ejms-2019.v4i1-527

[27] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

verification measures must be paired with robust security systems to protect users against hackers and other cyberattacks.

Vietnam adopted the Cybersecurity Law in 2018. It aims to ensure that activities in cyberspace do not harm national security, public order, or the lawful rights and interests of any organization or individual. This Law establishes fundamental rules that aim to enhance the safety and security of activities carried out in cyberspace. At the same time, Chapter III of this Law sets out rules on the prevention and actions against cybersecurity violations and regulates cybersecurity protection activities to create a secure internet environment. It also assures human resources for cybersecurity protection. However, these regulations are general and provide overall guidance; they do not specify particular violations or establish sanctions for such violations. Until 2022, Decree No. 53/2022/ND-CP on Elaborating Some Articles of The Law on Cybersecurity of Vietnam was issued and partially addressed some difficulties in implementation by authorities.

Thus, information in cyberspace will be monitored by competent authorities to promptly address fake news, misinformation, defamatory content, and the disclosure of others' private information, etc. However, this may lead to restrictions on the right to freedom of expression, especially when the State seeks to shape public opinion. For example, one dimension of this freedom is the right to seek and receive information. In certain situations, the State may apply the Cybersecurity Law as a means to restrict the public's access to information. As a result, individuals may be unable to obtain sufficient and accurate information or to gain a comprehensive understanding of an issue. In some cases, persons who expose shortcomings within the governmental system or criticize particular State policies may be blocked or even sanctioned. Such practices may infringe the freedom to hold opinions or to convey information that is essential for ensuring a democratic and rule of law principle. These actions may stem from vested interests or from attempts by individuals or groups in positions of authority to conceal wrongdoing.

IV. Artificial Intelligence and Non-discrimination

The fourth industrial revolution introduced disruptive technologies like big data and artificial intelligence[28]. These show the most remarkable achievements in modern technological progress. AI, in particular, possesses faster and more accurate analysis capabilities than humans. It can process huge amounts of data in a short time to examine, analyze, and generate effective recommendations. Moreover, AI has professional language skills that enable it to understand and translate into many

[28] Zhisheng Chen, 'Ethics and Discrimination in Artificial Intelligence - Enabled Recruitment Practices', Humanities and Social Sciences Communications (2023) 567. 1. https://doi.org/10.1057/s41599-023-02079-x

different languages. These features make AI an intelligent and versatile tool that supports human activities across virtually all sectors.

AI systems have had a significant impact on most aspects of life, particularly as generative AI is capable of producing new data outputs that shape subsequent processes. Meanwhile, the nature of generative AI relies on collected data and the use of algorithms, as well as user-provided prompts, to generate answers, predictions, new products, or proposed solutions. Its outputs depend largely on the quality, accuracy, and diversity of the data on which it was trained, as well as the way prompts are formulated. Therefore, in some cases, AI systems may produce results that are biased or discriminatory because there are various subjective and objective reasons for this. It rises to harmful bias and discrimination with risks to individuals, communities, or societies. These issues may stem from incomplete or inaccurate training data, unclear prompts, the subjective intentions of those who train the AI, or errors in training data processing.

Researchers and technologists have repeatedly demonstrated that algorithmic systems can produce discriminatory outputs.[29] Practically, when AI systems are used in employment management or in the recruitment and selection of personnel, their decisions can seriously affect the right to work of individuals and even their future career prospects. For example, AI applications used by Amazon as a recruiting tool have been found to discriminate based on gender.[30] Besides, when AI systems are used as supporting tools in education or in the workplace, faulty algorithms that generate biased or discriminatory outputs can lead to unfair treatment and create misguided tendencies for a specific group of people. Furthermore, a system in the United States used to assess the risk of reoffending within the criminal justice system was found to discriminate on the basis of race. This system predicted that people of color may reoffend almost twice compared to white persons.[31] In short, any negative impacts are likely to broaden in scale and scope.

In Vietnam, there is no independent document regulating discrimination in technology and AI. This issue is combined in several legal sectors. First, Article 16 of the 2013 Constitution of the Socialist Republic of Vietnam provides that all people are equal before the law. No one is subject to discriminatory treatment in political, civil, economic, cultural, or social life. Moreover, Article 26 claims that male and female citizens have equal rights in all fields. The State shall adopt policies

[29] Chiraag Bains, 'The legal doctrine that will be key to preventing AI discrimination' (*Brooking*, 13 September 2024) https://www.brookings.edu/articles/the-legal-doctrine-that-will-be-key-to-preventing-ai-discrimination/ accessed 05 November 2025

[30] More referrence: Jeffrey Dastin, 'Insight - Amazon scraps secret AI recruiting tool that showed bias against women' https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ accessed 15 October 2025.

[31] Bach Duong, 'The impact of artificial intelligence' (*Nhandan,* 28 March 2024) https://nhandan.vn/tac-dong-cua-tri-tue-nhan-tao-post802055.html accessed 10 November 2025

to guarantee the right to and opportunities for gender equality. The State, society, and family shall create the conditions for women to develop comprehensively and to advance their role in society. All gender discrimination acts are prohibited. This is reclaimed in the 2006 Law on Gender Equality, which aims to highlight and implement this rule in specific fields, such as politics, economy, labour, education, and technology. The 2019 Labor Code, the 2010 Law on Persons with disabilities, the 2019 Education Law, etc, also provide rules on prohibiting discrimination.

Overall, the current regulations are quite general and fragmented across multiple legal domains and specialized legislative areas. When identifying AI-driven discrimination and implementing measures to combat it, there is no unified definition, and regulations are governed by many legal domains. This leads to different interpretations among authorities or even a shifting of responsibility among them. This fragment creates a challenge in effectively enforcing these regulations.

Meanwhile, in the EU, 2024 marked a significant milestone with the adoption of the world's first AI Act. This Act provides a solid foundation when creating a uniform legal framework for the development and use of AI systems in the Union. As Recital 56 of this Law, if AI systems are improperly designed and used, these may be intrusive and may violate the right not to be discriminated against and perpetuate historical patterns of discrimination, for example, against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. Therefore, the AI Act requires providers to implement appropriate safeguards to protect the fundamental rights and to comply with all applicable conditions for high-risk AI systems. These obligations aim to ensure the quick detection of bias and discrimination. On the other hand, training, validation, and testing data are vital elements in the development of high-risk AI systems, and therefore, they must be subject to strict data governance and management practices. Therefore, under Article 10 of this Act, one of these is an examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights, or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations.

Thus, the AI Act sets out a classification framework for AI systems in order to ensure that risk-appropriate governance measures are applied. It also establishes specific requirements for high-risk AI systems to mitigate misuse and to reduce bias and discrimination. With risk prevention methods and the clarification of obligations of providers, this Act facilitates the robust development of AI and ensures cybersecurity. It is not only a precondition for building trust among developers and users, but also an effective support tool for socio-economic development.

In conclusion, the remarkable development of technology has transformed cyberspace into an integral part of human life. The number of activities that take place within cyberspace or are closely connected to it is increasing. Therefore, the protection of human rights can not be limited to the physical world but must also be expanded into cyberspace. From this perspective, transparency may serve as a cross-cutting guarantee of rights protection, since it connects the accessibility of legal norms, the accountability of public authorities and the effective exercise of individual rights.[32] Vietnam and many other countries have been proactively developing and implementing specific regulations to protect human rights in technological development. Meanwhile, the EU has established a solid and comprehensive legal framework for human rights protection. Studying the EU's experience and assessing Vietnam's current legal framework will help identify appropriate pathways to improve human rights protection. This plays a vital role in the country's development and integration process.

STATEMENTS

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

The author received no financial support for the research, authorship, or publication of this article.

Data deposition and availability

There is no data set associated with the study. No data deposition was required for this study.

Use of Artificial Intelligence

The author did not use any artificial intelligence system in the preparation of this article.

Author contributions (CRediT)

Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.

[32] Balázs Hohmann, *Az átláthatóság értelmezése és követelményrendszere a közigazgatási hatósági eljárások tükrében* [The Interpretation and Requirements of Transparency in Administrative Authority Proceedings] (Novissima Kiadó 2022) 271.