International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Law on the Protection of Women's Sensitive Personal Data in the Digital Environment: Current Gaps and Policy-Oriented Recommendations

Quynh Hoa Duong

Institute of State and Law, Vietnam Academy of Social Sciences, Vietnam
Corresponding Author Email: *dqhoa77[at]gmail.com*

Abstract: ***In the digital era, protecting women's sensitive personal data is a pressing need to ensure their privacy, honor and safety. The Law on Personal Data Protection 2025 has created a unified legal framework for this field, but there are still many limitations: lack of specialized regulations associated with gender, sanctions are not enough deterrent, compensation and remedy mechanisms are weak, and the responsibilities of cross-border platforms are not clear. The article uses the approach of human rights, gender and legal comparison to analyze the current situation of Vietnamese law, compare it with international standards, and on that basis propose to improve the law in the direction of gender sensitivity and high enforceability. Protecting women's sensitive personal data is therefore not only a legal requirement but also a protection of human dignity and rights in a digital society.***

Keywords: sensitive personal data, personal data protection, women, personality rights

1. Introduction

In the context of the global strong transition to the digital economy, personal data has become a particularly valuable asset that is likened to the "new source of oil" of the 21st century. The exploitation, processing, and storage of personal data not only brings enormous socio-economic benefits, but also poses a potential risk of infringing on privacy and human dignity on an ever more profound scale. Specially, women's sensitive personal data is becoming the most vulnerable target in the digital era. When such data is illegally obtained or disclosed, women often suffer more severe consequences than men, not only in terms of honor, dignity, and psychology, but also in terms of career opportunities, social status, and personal safety.

The UN Women report shows that women and girls experience at least one form of violence or online harassment ranging from 16% to 58% depending on the survey area, with the most common forms being disseminating images, illegally sharing personal information and infringing on honor on social networking sites[1]. Another study by UN Women in the Arab region (2021) found that 60% of women using the Internet experienced online violence in the survey year[2]. These figures show that protecting women's sensitive personal data is not only an administrative concern but a fundamental human rights issue and gender equality in the digital age.

Faced with that situation, the Law on Personal Data Protection 2025 has marked an important step in establishing a unified legal framework for the field of personal data protection in Vietnam. However, current regulations still lack specialized content associated with gender factors and do not have an appropriate protection mechanism for women, the group most at risk in the digital space.

From that context, this presentation was chosen with the main goal of clarifying the concept of women's sensitive personal data in the digital environment, clearly identifying gaps in the current law, and proposing solutions to improve the law on the protection of women's sensitive data in Vietnam in accordance with gender characteristics and international trends.

2. Research Methods

The article is based on the methodology of dialectical materialism and historical materialism, combined with the approach to human rights and gender equality in modern legal science. From a legal perspective, the study examines the protection of women's sensitive personal data not only as a matter of data governance, but also as a concrete manifestation of ensuring human rights in the digital environment.

The article uses several key approaches as follows:

Human rights approach: considering the protection of personal data as a component of the right to protect privacy, personal secrets, honor and dignity as enshrined in the 2013 Constitution and international treaties to which Vietnam is a signatory.

Gender approach: emphasizing the peculiarities of women in the protection of personal data, thereby pointing out the need to develop a gender-sensitive legal mechanism.

[1] UN Women (2022), *Accelerating efforts to tackle online and technology-facilitated violence against women and girls*, https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf accessed on October 9th, 2025.

[2] UN Women (2024), Creating safe digital spaces free of trolls, doxing, and hate speech, https://www.unwomen.org/en/articles/explainer/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech, Accessed on October 9th, 2025.

Regarding research methods, the article uses a synthesis of traditional research methods in legal science, specifically as follows:

- Methods of analysis and synthesis used to systematize the concepts, principles and legal regulations on sensitive personal data, thereby summarizing the theoretical basis for the research problem.
- Methods of legal comparison, applied when comparing the provisions of the Law on Personal Data Protection 2025 with international standards and laws of some typical countries, aims to identify gaps and trends in improvement.
- Induction and interpretation methods, in order to draw general judgments from specific data and propose orientations for improving the law.

Additionally, the article also exploits secondary materials from official sources such as legal documents, reports of state agencies, studies by UN Women, the OECD, the European Union, and scientific articles both domestic and international. The combination of the above methods helps to ensure the objectivity, comprehensiveness and practical applicability of the research results.

3. Results and Discussion

3.1 Overview of the protection of women's sensitive personal data in the digital environment

In the digital age, "personal data" is regarded an essential resource for all governance, economic and technological activities. According to the Organization for Economic Co-operation and Development (OECD) on protecting privacy and personal data among nations, personal data refers to any information relating to or enabling the identification of a specific individual[3]. This OECD provision is merely a recommendation, but it is widely recognized and adopted by many countries worldwide today. Both legal frameworks and international scholars concur that personal data encompasses all information pertaining to an identifiable individual, either directly or indirectly. Personal data includes not only clearly identifiable information such as full name, identification number, or facial features, but also digital footprints like access behavior, location, transaction history, and device data, if such information allows for the inference or identification of a specific individual.

In the scope of personal data, "sensitive personal data" is considered as the most vulnerable component of personal information. Sensitive personal data refers to information which, if processed, disclosed, or inferred unlawfully, would directly affect the dignity, honor, health, safety, or legitimate interests of the individual concerned. Article 9 of the European Union's General Data Protection Regulation (GDPR, 2016/679) refers to this group as special categories of personal data[4]. The processing of these data is prohibited, except for a few narrow exceptions such as with the explicit consent of the data subject, for reasons of substantial public interest, or for medical, social welfare or scientific research purposes.

Approaching that international trend, in Clause 3, Article 2 of the Law on Personal Data Protection 2025 of Vietnam, it is determined: *Sensitive personal data is personal data associated with the privacy of individuals, when infringed, it will directly affect the legitimate rights and interests of the subject.* Compared to Decree No. 13/2023/ND-CP on Personal Data Protection (hereinafter referred to as Decree No. 13/2023), the definition in the Law on Personal Data Protection 2025 demonstrates a risk-based and legal consequence-based approach, rather than merely listing items in a enumerative list as in Decree No. 13/2023.

For women, sensitive personal data possesses specific gender-related characteristics. Lots of types of information, although structurally similar between the two genders, demonstrate in practice that women experience a higher degree of vulnerability when such data is infringed, particularly in the context of existing societal prejudices. For example, the publicity of women's private images or reproductive health information often leads to more serious consequences than men.

Hence, women's sensitive personal data can be understood as deeply private information which, if unlawfully disclosed or exploited, would cause particular harm to women's honor, dignity, health, psychological well-being and social standing. This category of data includes information on reproductive health, personal images, biometric data, marital life, family relationships, and sexual orientation. The protection of this data category is also linked to the principle of gender equality, affirmed by the 2013 Constitution and the CEDAW Convention, pursuant to which the State has an obligation to eliminate prejudices and customary practices based on notions of inferiority or superiority of either sex.

On the basis of the above concept, it can be understood that the protection of sensitive personal data is the whole of legal, technical and organizational measures to ensure that sensitive data is only processed legally, safely and under the control of the data subject. In the digital environment, this concept not only includes information security but also the entire process of data processing from collection, storage, use, sharing, to deletion.

The approach of the GDPR (Article 9) and many modern legal systems are based on the principle: the processing of sensitive data is prohibited, unless there are clear legal grounds and special safeguards[5]. Vietnam's Personal Data Protection Law 2025 has also approached this spirit when it stipulates the requirement for separate consent, data impact assessment

[3] OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed on October 10th, 2025.

[4] Art. 9 GDPR Processing of special categories of personal data, https://gdpr-info.eu/art-9-gdpr/ Accessed on October 9th, 2025.

[5] APEC Privacy Framework (2005), Published by APEC Secretariat, https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, accessed on October 9th, 2025.

(DPIA)[6] and the obligation to notify[7] regulators when processing sensitive data.

For women, protecting sensitive data in the digital environment holds significance beyond technical frameworks, serving as a measure to safeguard dignity and prevent gender-based digital violence. When reproductive health data, medical records, private images or biometric data are leaked, it not only violates data rights but also leads to psychological harm, damage to honor and inequality of opportunity. Protecting women's sensitive personal data in the digital environment is not merely a legal requirement but also a humanitarian strategy to ensure that women can participate, innovate, and thrive in the digital space safely, equally, and with respect for their dignity.

3.2 The current situation of the law on women's sensitive personal data protection in the digital environment in Vietnam

The right to protect private life and personal secrets is one of the fundamental personal rights of human beings, widely recognized by Vietnamese and international law. Article 21 of the 2013 Constitution affirms: *"Everyone has the inviolable right to private life, personal secrets and family secrets; information about private life, personal secrets and family secrets is safeguarded by law"*. This is the constitutional foundation for establishing a legal framework regarding the right to control personal information, which is the core content of the concept of personal data protection.

On the basis of that constitution, Article 38 of the Civil Code 2015 clearly stipulates that the collection, storage, use and disclosure of information related to the private life of an individual must be agreed by that person, unless otherwise provided for by law. Within the Vietnamese legal system, Decree No. 13/2023 for the first time introduced clear legal definitions for "personal data" and "sensitive personal data" (Clause 4, Article 2). Subsequently, the Law on Personal Data Protection 2025 officially elevated the legal framework from a decree to a law, establishing a unified, comprehensive regulatory system concerning principles, rights, obligations, and data protection mechanisms. A novel aspect of the 2025 Personal Data Protection Law is its risk-based approach, a modern legislative paradigm adopted by numerous nations, which determines the "sensitivity" of data based on its potential impact on human rights. The law not only protects static information but also governs the entire data processing lifecycle. The Law further establishes higher security standards for sensitive data, approaching the benchmarks of GDPR (EU). Notably, the Law recognizes the rights to be informed, consent, access, rectification, erasure, and object to data processing, thereby empowering individuals, particularly women, with legal instruments to control and protect their sensitive information within the digital environment.

However, from a practical perspective, the current framework for protecting sensitive personal data still leaves many gaps.

Firstly, from a gender perspective, the 2025 Law on Personal Data Protection has yet to include specific provisions for women and other vulnerable populations.

Many types of data related to women, such as reproductive health, marital status, sexual orientation, or private imagery, carry a much higher level of risk than data from other groups. The unauthorized disclosure, exploitation or use of such information not only infringes upon personal data rights but may also result in reputational harm, social stigmatization, and gender-based violence. Practice in Vietnam shows that the infringement of sensitive personal data of women is increasingly sophisticated and complicated. Incidents involving the dissemination of private images and videos, the use of deepfake technology for image fabrication, or the sharing of medical and reproductive health data without consent are occurring with high frequency[8]. According to the Ministry of Public Security, in recent years, the illicit collection, appropriation and trafficking of personal data, including sensitive data[9], have rapidly escalated[10], with thousands of cases discovered annually; however, only a minor proportion of these cases are detected and duly processed. Many infringing acts transpire on cross-border platforms, rendering legal enforcement and the attribution of responsibility nearly impossible. Women constitute the demographic most severely affected by this predicament. A 2022 report by UN Women indicates that over half of women globally who use the Internet have experienced at least one form of online violence, with the most prevalent forms being the disclosure of personal information and the dissemination of private images[11]. In Vietnam, numerous instances involve the exploitation of private images for blackmail or defamation, yet victims often elect to remain silent due to apprehension of social stigma.

A notable trend in many countries today is the integration of gender factors in personal data protection policies. The European Union has promulgated the "Gender Equality Strategy in the Digital Age" (2020–2025)[12], which mandates

[6] See Articles 21 and 22 of the Law on Personal Data Protection 2025.
[7] Article 23 of the Law on Personal Data Protection 2025.
[8] Van Anh (2025). *Recurring the trick of using Deepfake technology to fake videos and images to scam,* Vietnamnet, https://vietnamnet.vn/tai-dien-chieu-tro-dung-cong-nghe-deepfake-gia-mao-video-hinh-anh-de-lua-dao-2374468.html accessed on October 9th, 2025.
[9] Quy Nguyen (2023). *Detecting a large amount of personal data illegally collected and traded*, https://lsvn.vn/phat-hien-gan-1-300-gb-voi-hang-ti-du-lieu-ca-nhan-bi-thu-thap-mua-ban-trai-phep-1686148396-a131335.html, accessed on October 9th, 2025.
[10] Thu Hang (2025). *Closing the "loophole" to protect personal data in the digital age*, Nhan Dan Newspaper online, https://nhandan.vn/bit-lo-hong-bao-ve-du-lieu-ca-nhan-trong-thoi-dai-so-post875389.html, accessed on October 9th, 2025.
[11] UN Women (2022), *Accelerating efforts to tackle online and technology-facilitated violence against women and girls*, https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf accessed on October 9th, 2025.
[12] European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Union of Equality: Gender Equality Strategy 2020-2025, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0152 Accessed on October 9th, 2025;

technology agencies and enterprises to conduct gender impact assessments when processing sensitive data, particularly biometric and health data. The processing of "special categories" of data is absolutely prohibited unless there exists a clear legal basis; infringing organizations may incur penalties of up to 4% of the company's global turnover[13]. Japan has also added a similar requirement in the 2022 APPI implementation guidelines, which aim to ensure women are not discriminated against by biased algorithms or data collection practices[14]. In the Personal Information Protection Act of Japan (APPI, amended in 2020)[15], there is a separate provision for "information requiring special attention", stipulating that the data handler must provide clear notification and obtain separate consent from the data subject, while also establishing an independent supervisory authority[16]. This is the experience that Vietnam needs to study to design a mechanism to protect sensitive personal data in the direction of respect for dignity and gender equality, ensuring that data protection is not merely a technical concern but also a fundamental means of safeguarding individuals in the digital environment.

Secondly, the current mechanism for handling administrative and civil violations for acts of infringing sensitive personal data in the digital environment is not enough deterrent.

Regarding administrative sanctions, Decree No. 15/2020/ND-CP (as amended by Decree No. 14/2022/ND-CP) stipulates a fine ranging from VND 40-60 million for acts such as: using personal information for purposes other than those agreed upon or without consent; providing, sharing or disseminating personal information to a third party without consent; and unlawfully collecting, using, disseminating or trading personal information. This fine level is deemed excessively low compared to the severe nature of violations involving systemic or commercial exploitation of data, particularly when sensitive data can be extensively exploited in cyberspace.

Regarding civil sanctions, the Civil Code 2015 allows individuals to demand compensation for damages, correction, and apology when their honor, dignity, or reputation is infringed (Article 592). Nevertheless, current law lacks specific guidance on quantifying moral damages in cases of sensitive data leaks, resulting in actual compensation levels that are modest compared to the extent of harm suffered. Personal data in cyberspace exists as information, characterized by its intangible nature; though perceptible, it lacks a definitive physical form. In fact, no legal basis or precedent exists for valuing personal data for the purpose of compensation in lawsuits in Vietnam.

Thirdly, the criminal law does not provide for an independent crime of infringement of personal data, especially sensitive personal data.

While countries with developed digital economies have criminalized data infringement very early on and consider it a crime that violates human rights in cyberspace, in Vietnam, similar acts are currently still handled indirectly through adjacent offenses such as The Offense of Infringing upon the Secrecy or Safety of Mail, Telephones, Telegrams, or other Forms of Private Communication of Others (Article 159), or The Offense of Illegally Spreading or Using Information on Computer Networks, Telecommunication Networks (Article 288) within the Penal Code 2015, amended in 2017.

Practice shows that cases related to the dissemination of private images and videos or the leakage of information about women's health and personal life are often handled in the direction of insulting the honor and dignity or spreading depraved cultural products, rather than from the perspective of personal data infringement. This not only diminishes deterrent efficacy but also obscures the true nature of sensitive data infringement, an act that simultaneously violates human rights and harms network security and order. The absence of a specialized offense makes prosecuting authorities confused in categorizing crimes, readily leading to situations of confusion, overlap, or the omission of acts dangerous to society

Besides, criteria regarding "serious consequences" or "causing negative public opinion" in Article 288 have not been concretized, causing difficulties for prosecuting authorities in categorizing crimes and determining penalties, especially when the damages primarily involve emotional distress, honor, and dignity of women. In addition, criminal law does not yet stipulate the liability of legal entities in cases of data leaks due to insufficient security or internal collusion- a significant gap in the context where organizations and digital platforms increasingly hold vast amounts of personal data.

Fourthly, there is a lack of clarity on the civil compensation mechanism and remedial measures when violations occur.

The Law on Personal Data Protection 2025 only stipulates the general principles of the right to claim compensation, while there are no specific guidelines on the scope of damages, calculation methods and levels of compensation for damages. This leads to the data subjects' rights, especially those of women and other vulnerable groups susceptible to harm concerning honor and morale, not being fully guaranteed in practice.

International experience indicates that lots of nations consider civil compensation a cornerstone in personal data protection mechanisms, serving both to restore the rights of infringed individuals and to impose accountability upon data processors. For example, Act on India's Information Technology 2000 stipulates that organizations and enterprises must compensate for damages caused to others due to a lack

[13] GDPR Local (20250, Comparing GDPR with Asia's Data Protection Legislation https://gdprlocal.com/comparing-gdpr-with-asia-data-protection-legislation/.

[14] https://calawyers.org/privacy-law/japan-amends-its-privacy-law-with-important-changes/ Accessed on October 9th, 2025;

[15] Personal Information Protection Commission (2020), Amended Act on the Protection of Personal Information https://www.ppc.go.jp/files/pdf/APPI_english.pdf.

[16] Data Protection in Japan: All You Need to Know about APPI, https://www.endpointprotector.com/blog/data-protection-in-japan-appi/ Accessed on October 9th, 2025;

of responsibility in data security[17]. The European Union also permits individuals to claim compensation for both material and non-material damages under the GDPR, thereby enhancing deterrence and ensuring fairness for victims[18].

Meanwhile, in Vietnam, the Civil Code 2015 only provides general provisions on the liability to compensate for damages when civil rights are infringed, and does not recognize the right to personal data as an independent moral right. Due to the absence of direct legal grounds, courts often infer from the rights to honor, dignity, or private life, resulting in inconsistent application and widely divergent levels of compensation for moral damages. Consequently, women, the group enduring the most severe moral harm when sensitive data is compromised, still lack a sufficiently robust legal mechanism for fair compensation and protection.

Fifthly, the current law does not clearly stipulate the legal responsibilities of digital platforms, especially cross-border services, where the majority of data breaches are concentrated.

This is the area where the most data breaches occur, but it is also the most difficult to control, because most of the platforms that collect, analyze and exploit Vietnamese user data are operated from outside the national territory. Social media platforms, mobile applications, cloud storage services, and e-commerce platforms currently process enormous volumes of user data, including substantial sensitive data pertaining to women such as images, location information, health data, private communication content, and online behavioral patterns. Each upload, interaction, or share results in a quantity of personal data automatically collected and analyzed by the system for purposes such as advertising, content personalization, or user behavior identification. However, the Law on Personal Data Protection 2025 only stipulates the general obligations of data processors, but there is no specific enforcement mechanism for cross-border platforms and entities that do not have a legal presence in Vietnam.

As a result, when a breach occurs, it is almost impossible to ask these platforms to remove content, provide information, or coordinate investigations. Domestic data management authorities can only send administrative requests or diplomatic notes, while the platforms often invoke jurisdictional regulations, the data protection laws of their host countries, or their own policies to decline. This leaves women, the group most affected by the spread of sensitive data, almost without effective legal tools to protect them.

This gap also shows the lack of synchronization between Vietnamese law and international standards. In the European Union, the Digital Services Act (DSA, 2022) has clearly defined the legal obligations of large online platforms: they must have legal representatives in each member state, establish a mechanism for reporting violations, remove sensitive content within a short timeframe, and be accountable to data management authorities. GDPR 2016/679 also clearly stipulates that non-EU businesses collecting user data within the bloc must designate a "data representative" in the EU in order to ensure supervision and handle complaints[19]. In Singapore, the amended PDPA Act 2020 requires all foreign organizations providing services to Singaporean citizens to comply with equivalent data protection standards and to be responsible for all personal data processing activities originating within the territory[20].

Meanwhile, Vietnam's Law on Personal Data Protection 2025 has not yet established a similar mechanism. The Law does not clearly stipulate that foreign enterprises must have a data representative in Vietnam, nor does it define the obligation to respond to requests for data removal or provision within a specified period, and it lacks an official international cooperation mechanism between Vietnam's data management authority and data protection authorities of other countries. This makes it difficult for the domestic legal system to exert effective pressure on global platforms such as Facebook, TikTok, Instagram, Google or dating applications, where acts of spreading or collecting women's sensitive data occur most regularly.

The problem becomes especially serious when content infringes on women's sensitive data, such as private images illegally shared or manipulated using deepfake technology, can spread within minutes and surpass the control capabilities of all functional authorities. At that time, an administrative handling order or decision to prosecute in the country is no longer fast enough and enough to prevent the consequences. Victims, typically women, are rendered helpless, while the infringing party or the intermediary platform is still innocent because it is outside the jurisdiction of Vietnamese law.

Obviously, the fact that the Law on Personal Data Protection 2025 does not clearly stipulate the legal responsibilities of cross-border digital platforms is a major legal gap in the protection of personal data in general and the protection of sensitive data of women in particular. This gap not only diminishes the effectiveness of legal enforcement but also places women in an unequal position in cyberspace, where their data rights can be violated without a commensurate redress mechanism.

3.3 Solutions to improve the law on women's sensitive personal data protection in the digital environment

[17] Section 43A, Act on India's Information Technology 2000
[18] Article 82, GDPR (2016/679)
[19] VeraSafe (2024), EU Digital Services Act: Role of the Legal Representative, https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf, accessed om 10/10/2025; Latham & Watkins (2023), The Digital Services Act: Practical Implications for Online Services and Platforms, https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf, Accessed on October 20th, 2025.
[20] PDPC, Data Protection Obligations, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations, Accessed on October 10th, 2025; Peter Oladimeji (2023), Singapore Personal Data Protection Act (PDPA): all you need to know, Didomi Blog, https://www.didomi.io/blog/singapore-data-protection-pdpa-all-you-need-to-know? Accessed on October 20th, 2025.

First, perfecting the legal framework in the direction of specialization, gender sensitivity and approaching international standards.

The Law on Personal Data Protection 2025 is an important foundation, but remains framework-oriented. Thus, the guiding documents for implementation must be built to specialize in women's sensitive personal data. The list of sensitive personal data issued by the Government should specifically identify data categories linked to gender-specific characteristics such as reproductive health information, private images, marital status, sexual orientation or biometric data capable of revealing gender. For these categories, the highest level of protection must be applied: requiring separate, clear, and demonstrable consent; limiting processing purposes; mandating a data protection impact assessment before processing; and incorporating a gender impact assessment element into the general impact assessment process. At the same time, gender equality and human rights elements must be integrated into the Law's enforcement, drawing lessons from the experiences of the European Union (EU), Japan and Singapore, where data policies require authorities and technology enterprises to assess the risk of gender discrimination or harm to women's honor when processing sensitive data. This approach assists Vietnam not only in protecting information but also in safeguarding the dignity and autonomy of women in digital life.

Second, strengthening the effectiveness of sanctions and criminalize acts of infringement of sensitive personal data.

In order to overcome the lack of crimes, light sanctions and lack of deterrence, upgrading the framework for handling violations in all three fields of criminal, administrative and civil is necessary.

Firstly, in terms of criminality, it is recommended to study additional crimes of infringing personal data in the Criminal Code, with aggravating framing circumstances when the infringed object is sensitive data or when the victim is a woman and a vulnerable subject. Concurrently, provisions for the criminal liability of legal entities must be stipulated for instances of data leaks resulting from lax management, inadequate security measures, or illicit gains derived from processing personal data.

Secondly, in terms of administrative sanctions, the maximum fine level for sensitive data processing rule violations should be raised, and a penalty mechanism should be applied according to the proportion of domestic revenue, similar to the GDPR (EU) or PDPA (Singapore) model, to ensure deterrence. In addition, it is necessary to stipulate additional measures such as suspension of data processing, forced removal of data, or public apologies to victims.

Thirdly, in terms of civil liability, it is vital to have uniform guidance for the court when adjudicating cases of personal data infringement, especially on electronic evidence, the scope of joint liability and the time limit for emergency handling.

Third, clarifying the legal responsibilities of digital platforms, especially cross-border services.

The Personal Data Protection Law 2025 needs concretizing with clear obligations for cross-border platforms, which account for a large proportion of infringements. The law should require foreign enterprises to have a legal representative in Vietnam if they provide services involving the collection, analysis or processing of Vietnamese user data. This representative shall be responsible for coordinating with state agencies in receiving content removal requests, providing evidence, restoring data, or resolving complaints. Simultaneously, the law must regulate mandatory response deadlines and strong sanctions if platforms fail to comply. Besides, it is necessary to establish a framework for international cooperation on data protection, in the form of bilateral agreements or participation in regional mechanisms to strengthen the capacity to trace and handle cross-border sensitive data infringements.

Fourth, improving the mechanism for compensation for damage and remedy consequences.

In order to close the protection cycle, the law needs to develop a mechanism for compensation and substantive remedies for women who suffer from sensitive data breaches. First of all, it is necessary to standardize the basis for determining damage, in which non-material damage is recognized as a mandatory constituent factor. For sensitive data, especially private images or health data, the principle of presumed moral damage should be applied to alleviate the burden of proof on victims. Besides, it is vital to supplement non-financial remedies such as the right to request complete data deletion, removal of information from search results, public apologies and rectifications, or free psychological and legal support for infringed women. These measures not only compensate for damages but also carry significant symbolic value: affirming the State's respect for and protection of women's dignity in the digital space.

4. Conclusion

In the context of far-reaching digital transformation, personal data has become a new form of “power asset” of human, associated with honor, dignity and personal freedom. Protecting women’s sensitive personal data is not only a technical requirement in information governance, but also a human rights and gender equality issue in the digital society.

The Personal Data Protection Law 2025 has opened a specialized legal framework for this field, yet to be truly effective, Vietnamese law needs improving in the direction of specialization, gender sensitivity and high enforceability. This includes criminalizing personal data infringement, strengthening deterrent sanctions, establishing a speedy procedural mechanism, clearly defining the responsibilities of digital platforms, and developing a compensation and remediation mechanism suitable for gender characteristics.

Only when legal measures are operated in sync with raising social awareness will women be truly empowered to control information about themselves and be protected from invisible but profound trauma in the online world. Therefore, protecting women's sensitive personal data is protecting human dignity and rights in the digital age.

References

[1] APEC Privacy Framework (2005), Published by APEC Secretariat, https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf.
[2] Art. 9 GDPR Processing of special categories of personal data, https://gdpr-info.eu/art-9-gdpr/.
[3] Bui Si Thanh & Tran Thi Diu (2025). *Law on initiating a lawsuit against personal data infringement in cyberspace: Limitations and several recommendations, Legal e-Magazine*, https://phaply.net.vn/phap-luat-ve-khoi-kien-vu-an-xam-pham-du-lieu-ca-nhan-tren-khong-gian-mang-han-che-va-mot-so-kien-nghi-a259905.html.
[4] Data Protection in Japan: All You Need to Know about APPI, https://www.endpointprotector.com/blog/data-protection-in-japan-appi/.
[5] European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Union of Equality: Gender Equality Strategy 2020-2025, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0152.
[6] GDPR Local (20250, Comparing GDPR with Asia's Data Protection Legislation https://gdprlocal.com/comparing-gdpr-with-asia-data-protection-legislation/.
[7] Latham & Watkins (2023), The Digital Services Act: Practical Implications for Online Services and Platforms, https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf.
[8] *Morgan Lewis (2022),* Singapore Personal Data Protection Act Changes Have Implications for Healthcare Sector, https://www.morganlewis.com/pubs/2022/08/singapore-personal-data-protection-act-changes-have-implications-for-healthcare-sector.
[9] OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[10] PDPC, Data Protection Obligations, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations.
[11] Personal Information Protection Commission (2020), Amended Act on the Protection of Personal Information, https://www.ppc.go.jp/files/pdf/APPI_english.pdf.
[12] Peter Oladimeji (2023), Singapore Personal Data Protection Act (PDPA): all you need to know, Didomi Blog, https://www.didomi.io/blog/singapore-data-protection-pdpa-all-you-need-to-know?
[13] Quy Nguyen (2023), *Detecting a large amount of personal data illegally collected and traded*, https://lsvn.vn/phat-hien-gan-1-300-gb-voi-hang-ti-du-lieu-ca-nhan-bi-thu-thap-mua-ban-trai-phep-1686148396-a131335.html.
[14] Thu Hang (2025). *Closing the "loophole" to protect personal data in the digital age*, Nhan Dan Newspaper, https://nhandan.vn/bit-lo-hong-bao-ve-du-lieu-ca-nhan-trong-thoi-dai-so-post8753Thu89.html accessed on October 9th, 2025.
[15] Minh Duc (2025), *Detecting more than 110 million records of personal data that have been traded,* Tien Phong Newspaper online https://tienphong.vn/phat-hien-hon-110-trieu-ban-ghi-du-lieu-ca-nhan-da-bi-mua-ban-post1758363.tpo.
[16] Law Library, *Convention on Eliminating All Forms of Discrimination Against Women, 1979*, https://thuvienphapluat.vn/van-ban/Linh-vuc-khac/Cong-uoc-ve-xoa-bo-moi-hinh-thuc-phan-biet-doi-xu-chong-lai-phu-nu-1979-269872.aspx.
[17] UN Women (2022), *Accelerating efforts to tackle online and technology-facilitated violence against women and girls*, https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf.
[18] UN Women (2024), Creating safe digital spaces free of trolls, doxing, and hate speech, https://www.unwomen.org/en/articles/explainer/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech.
[19] Van Anh (2025). *Recurring the trick of using Deepfake technology to fake videos and images to scam*, Vietnamnet https://vietnamnet.vn/tai-dien-chieu-tro-dung-cong-nghe-deepfake-gia-mao-video-hinh-anh-de-lua-dao-2374468.html.
[20] VeraSafe (2024), EU Digital Services Act: Role of the Legal Representative, https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf.