International Journal Of Management And Economics Fundamental

VOLUME Vol.05 Issue 09 2025
PAGE NO. 29-34
DOI 10.37547/ijmef/Volume05Issue09-05

Ensuring Information Security: Foreign Experience, Challenges, And Solutions

Mamatov Abror Alisherovich

Senior Prosecutor, Department for Public Relations and Legal Information, Office of the Prosecutor General, Uzbekistan

Received: 31 July 2025; **Accepted:** 28 August 2025; **Published:** 30 September 2025

Abstract: In the contemporary digital era, the growing dependence of individuals, societies, and states on information resources has significantly increased the urgency of ensuring information security. The rapid expansion of internet usage, accompanied by the proliferation of cybercrimes and emerging global threats, has created the necessity for states to modernize their legal frameworks and adopt international best practices. This article examines both the national efforts of Uzbekistan—particularly through the implementation of the Digital Uzbekistan – 2030 Strategy—and comparative experiences from Germany, Russia, and Estonia. The German Network Enforcement Act (NetzDG), Russia's amendments to its Law on Information, and Estonia's criminal liability for the unauthorized disclosure of professional secrets are analyzed as illustrative models of foreign approaches to safeguarding information security. The study identifies existing shortcomings in Uzbekistan's current legal framework, such as the vulnerability of government web resources, the absence of a unified legislative act governing information security, and the lack of a comprehensive legal definition of the concept. Finally, the paper proposes practical solutions, including the codification of an Information Code, the development of a clear and adaptive legal definition of information security, and the introduction of preventive legal measures to enhance the protection of governmental digital infrastructure. By integrating foreign experience and national reforms, Uzbekistan can strengthen its information security regime while ensuring consistency with evolving global standards.

Keywords: Information security; cyber threats; digital transformation; Uzbekistan; Digital Uzbekistan – 2030; NetzDG; Russia; Estonia; legal framework; information legislation; comparative law; cybercrime prevention.

Introduction: In the contemporary information age, meeting the growing demand for access to information has become a critical priority. The number of internet users worldwide has been increasing steadily each year, reflecting the profound digital transformation of societies. For instance, in Uzbekistan alone, the number of internet users rose dramatically from 14.7 million in 2017 to 32.7 million in 2025, marking an increase of more than 120 percent within less than a decade. This sharp rise underscores not only the expanding reliance on digital resources but also the necessity of ensuring their security alongside guaranteeing free access to information.

Information security has thus emerged as one of the most essential dimensions in safeguarding the interests of individuals, societies, and states. According to the International Telecommunication Union (ITU), global cybercrime damages are projected to cost the world economy USD 10.5 trillion annually by 2025, compared to only USD 3 trillion in 2015. The rapid advancement of information and communication technologies (ICT), the escalation of cybercrimes, and the emergence of cross-border digital threats have compelled states to both refine their national legislation and adapt to international standards.

The borderless nature of the digital environment further complicates this issue. Information can be transmitted across national boundaries instantly, with users in one state sharing or receiving data from another without geographical constraints. The rise of online platforms and transnational information flows highlights the urgency of reinforcing cybersecurity mechanisms and developing coordinated legal responses.

Uzbekistan has undertaken significant legislative and institutional measures to strengthen its national information security framework. A milestone initiative was the Presidential Decree No. 6079 of October 5, 2020, which approved the "Digital Uzbekistan – 2030" Strategy (President of the Republic of Uzbekistan, 2020). This strategic program emphasized not only the development of digital infrastructure but also the enhancement of digital literacy among public officials. In particular, the decree mandated that relevant higher education institutions provide training in ICT and information security to approximately 12,000 civil servants annually, with funding allocated from local budgets (President of the Republic of Uzbekistan, 2020).

Moreover, beginning November 1, 2020, all executive bodies were required to designate a deputy head responsible for digitalization. Among their core responsibilities is ensuring the protection of ministerial digital infrastructure, including the safeguarding of electronic data and official documents. In addition, the decree introduced measures for the further development of e-government services, including Article 29 of the Action Plan, which specifically requires strengthening information security within the Unified Interactive State Services Portal (President of the Republic of Uzbekistan, 2020).

These reforms demonstrate Uzbekistan's recognition that information security is not merely a technical issue but an integral component of governance, legal regulation, and national security in the digital era.

The legal and practical measures discussed above are not unique to Uzbekistan; many foreign countries have already implemented similar frameworks and, in some cases, have gone further by introducing additional mechanisms that remain untested in Uzbekistan. Therefore, studying international experience is both relevant and necessary to strengthen the national approach to information security.

One of the most illustrative examples is Germany's adoption of the Network Enforcement Act (NetzDG) in 2017. This law is considered a landmark step in ensuring information security and combating harmful online content. It obliges large social media platforms with more than two million registered users to develop effective mechanisms for reviewing complaints concerning illegal content, as defined under Section 22 of the German Criminal Code (Bundesministerium der Justiz und für Verbraucherschutz, 2017). According to the law, clearly unlawful content must be removed within 24 hours, while more complex or disputed cases may be extended up to seven days for further examination. To guarantee oversight, unresolved cases are referred to a special body under the Federal Ministry of Justice and Consumer Protection, which is mandated to deliver a final decision within seven days.

Failure to comply with the law carries significant penalties: corporations may face fines of up to EUR 50 million, while responsible officials can be fined up to EUR 5 million (European Commission, 2018). The adoption and enforcement of NetzDG marked a new stage in Germany's information security policy by addressing not only cyber threats but also the protection of national security, the dignity of citizens, and the integrity of personal data.

Empirical evidence indicates that Germany has seen a measurable reduction in the circulation of extremist and hate-driven content since the enforcement of NetzDG. For example, Facebook's Transparency Report revealed that content removals in Germany increased by 40% between 2018 and 2020 following the law's implementation (Facebook Transparency Report, 2020). The act effectively transformed social networks into "co-regulators," requiring them to act as responsible actors within the digital ecosystem, thereby balancing state security interests with commercial freedom.

From an information security perspective, NetzDG prevents the uncontrolled spread of disinformation, threats, extremist propaganda, and hate speech, which not only destabilize the digital space but also undermine social cohesion and public trust in mass media. Furthermore, the German model has been widely observed and, in some cases, adapted by other jurisdictions, making it a practical case study in the development of regulatory approaches to digital governance (Gorwa, 2019).

In recent years, the regulatory measures adopted in Russia to strengthen information security, particularly the legislative amendments that came into force in 2020, have been recognized as concrete steps aimed at ensuring the country's digital sovereignty. In particular, pursuant to the amendments to the Federal Law "On in Uzbekistan. Therefore, studying international experience is both relevant and necessary to strengthen the national approach to information security.

One of the most illustrative examples is Germany's adoption of the Network Enforcement Act (NetzDG) in 2017. This law is considered a landmark step in ensuring information security and combating harmful online content. It obliges large social media platforms with more than two million registered users to develop effective mechanisms for reviewing complaints concerning illegal content, as defined under Section 22 of the German Criminal Code (Bundesministerium der

Justiz und für Verbraucherschutz, 2017). According to the law, clearly unlawful content must be removed within 24 hours, while more complex or disputed cases may be extended up to seven days for further examination. To guarantee oversight, unresolved cases are referred to a special body under the Federal Ministry of Justice and Consumer Protection, which is mandated to deliver a final decision within seven days.

Failure to comply with the law carries significant penalties: corporations may face fines of up to EUR 50 million, while responsible officials can be fined up to EUR 5 million (European Commission, 2018). The adoption and enforcement of NetzDG marked a new stage in Germany's information security policy by addressing not only cyber threats but also the protection of national security, the dignity of citizens, and the integrity of personal data.

Empirical evidence indicates that Germany has seen a measurable reduction in the circulation of extremist and hate-driven content since the enforcement of NetzDG. For example, Facebook's Transparency Report revealed that content removals in Germany increased by 40% between 2018 and 2020 following the law's implementation (Facebook Transparency Report, 2020). The act effectively transformed social networks into "co-regulators," requiring them to act as responsible actors within the digital ecosystem, thereby balancing state security interests with commercial freedom.

From an information security perspective, NetzDG prevents the uncontrolled spread of disinformation, threats, extremist propaganda, and hate speech, which not only destabilize the digital space but also undermine social cohesion and public trust in mass media. Furthermore, the German model has been widely observed and, in some cases, adapted by other jurisdictions, making it a practical case study in the development of regulatory approaches to digital governance (Gorwa, 2019).

In recent years, the regulatory measures adopted in Russia to strengthen information security, particularly the legislative amendments that came into force in 2020, have been recognized as concrete steps aimed at ensuring the country's digital sovereignty. In particular, pursuant to the amendments to the Federal Law "On Information, Information Technologies, and the Protection of Information", large social media platforms were required to establish official representative offices in Russia. Through this measure, foreign platforms are expected to comply with local jurisdiction, thereby establishing effective control over the content disseminated through them. Under the new regulation, social networks are required to identify and independently block unlawful information on their platforms. This primarily concerns content that demonstrates disrespect toward the state and society, or that may incite social instability, such as calls for extremism, unauthorized assemblies, and public disorder. If a complaint is filed against specific content, access to it must be restricted within 24 hours.

In addition, the law provides a legal definition of the term "social network," which applies to any online platform operating within the Russian Federation that has a daily audience exceeding 500,000 users. This practice indicates that while the state seeks to strengthen its control over the information space, it simultaneously expands the scope of accountability for online platforms. Consequently, social networks are now required not only to disseminate content but also to filter it and ensure its compliance with established security standards. Although this approach has sparked international debate, it is increasingly recognized as an essential mechanism for ensuring information security, protecting citizens from information-related threats, and maintaining societal stability.

In many foreign jurisdictions, the disclosure of professional or service-related confidential information is treated as a criminal offense. For example, the Criminal Code of the Republic of Estonia provides a clear legal framework in this regard. According to Article 157, if an individual unlawfully discloses confidential information entrusted to them in the course of their professional or service duties—such as information relating to another person's health, private life, or commercial activity—they are subject to criminal liability. The legislation emphasizes that such information becomes known specifically in the performance of official or professional responsibilities, and where a legal duty of confidentiality applies, its disclosure constitutes not only an ethical breach but also a legal offense. This approach is regarded in Estonia as a fundamental component of information security, serving to ensure strict adherence to the principle of confidentiality.

An analysis of the existing legislative framework reveals that, despite the establishment of numerous legal foundations for ensuring information security, certain shortcomings remain. These issues may be considered one by one.

Issues.

First, one of the most vulnerable aspects of information security continues to be the websites of state bodies. This vulnerability may be explained by several factors: the use of outdated or insufficient technical protection tools, the relatively low level of professional competence among system administrators and IT

specialists, and the absence of well-developed policies, regulations, or rules on information security. As a result, such web resources remain exposed to cyberattacks.

This situation is clearly confirmed by statistical data from 2023. According to monitoring and analytical assessments conducted by the Cybersecurity Center of the Republic of Uzbekistan, a total of 1,186 vulnerabilities were identified across 677 web resources, of which 1,022 were found directly in the official websites of state bodies. Out of these vulnerabilities, only 587 were eliminated with the assistance of specialists, leaving the majority unresolved. This indicates that systemic weaknesses remain unaddressed (Cybersecurity Center of Uzbekistan, 2023).

Such vulnerabilities pose a serious threat not only to national information security, but also to the protection of citizens' personal data, the efficiency of public administration, and the overall level of trust in the state itself. This is despite the fact that the Presidential Decree "On Measures to Bring the Sphere of Information and Communication Technologies to a New Stage in 2022–2023" provides for several measures to enhance information security. Similarly, Clause 19 of the Regulation approved by the Resolution of the Cabinet of Ministers "On Improving the Operation of Official Websites of State Bodies and Organizations" requires that official websites maintained on the Unified Platform must comply with established information security standards.

Nevertheless, the above-mentioned circumstances indicate that there are still significant shortcomings in the enforcement of these legislative and regulatory provisions.

Second, Uzbekistan still lacks a single, universal piece of legislation regulating information and information security. Instead, this sphere is governed by a number of separate laws, each protecting information security in different ways. In some cases, these laws complement one another, but in others they duplicate the same provisions, which leads to redundancy and confusion. As a result, citizens often do not fully understand which law provides guarantees of their information security or which legal act they should invoke in particular situations.

For example, as previously noted, Article 11 of the Law "On the Principles and Guarantees of Freedom of Information" and Articles 19–20 of the Law "On Informatization" both contain provisions with identical content. The repetition of these norms not only increases the volume of legislation in this field but also complicates public understanding of the legal framework. Duplication undermines legislative clarity and has little practical value.

Moreover, while the rights and obligations of officially registered information resources are regulated under the Law "On Mass Media", there is still no principal act regulating the legal regime of unregistered information resources (although a draft has been prepared). At present, this area continues to be governed, to varying extents, by fragmented laws, by-laws, and ministerial regulations. Yet, given the rapid development of the sector and the expansion of related social relations, it is necessary to elevate the regulatory norms of this field to the level of law rather than relying mainly on subordinate acts.

Third, none of the laws currently in force provides a complete and precise definition of "information security." For instance, the Law "On the Principles and Guarantees of Freedom of Information" mentions the concepts of information security and security in the information sphere multiple times (three and thirteen references, respectively), yet offers only a brief definition in Article 3: "the state of protection of the interests of the individual, society, and the state in the field of information." The Law "On Informatization" provides no definition at all, and the Law "On Cybersecurity" defines only the narrower concept of cybersecurity. Thus, the broader notion of information security is left inadequately defined.

The absence of a comprehensive and uniform legal definition of information security creates problems for legal practice. Where a concept is open to multiple interpretations, state agencies, courts, law enforcement bodies, non-governmental organizations, and citizens may each understand and apply it differently. Such inconsistency inevitably results in confusion and the incorrect application of the law.

Furthermore, enshrining a precise definition of information security in legislation would facilitate the drafting of other relevant laws and regulations. For example, it would ensure consistency and coherence in areas such as the protection of personal data, the safeguarding of state secrets, and the security of digital infrastructure.

In addition, information security constitutes an integral part of national security, and legal uncertainty in this sphere could hinder the state's ability to implement a stable and coherent policy in the information domain. This is particularly critical in the context of cyberattacks on state infrastructure, emerging information threats, and weakened control over data flows, where clarity and precision in legal definitions are indispensable.

Finally, providing a clear, simple, and understandable legal definition of information security is essential to

raising the legal awareness of citizens and fostering a culture of information security. Citizens must be able to clearly recognize which actions constitute breaches of security and how they can protect themselves. For this reason, the introduction of a precise and comprehensive legal definition of information security is not only a legal necessity but also a practical and social imperative.

Solutions.

First, in order to reduce information threats to government web pages, it is necessary to introduce preventive measures directly into legislation. If such measures are not codified and threats are addressed only after they occur, the overall number of risks cannot be effectively reduced. Once a breach has taken place and information has been unlawfully accessed, restoring individual rights becomes extremely difficult, since the data may already have been disseminated or exploited for illicit purposes. Preventive measures could include the certification of specialists responsible for maintaining government web resources and the establishment of a mandatory professional attestation system in the field of information security at the legislative level.

Second, to strengthen legal regulation in the sphere of information, ensure coherence among normative legal acts, and eliminate contradictions arising in practice, it is essential to adopt a unified, comprehensive, and foundational legislative act—an Information Code.

At present, social relations in the field of information in the Republic of Uzbekistan are governed by a variety of separate laws and regulations. These include, inter alia, the laws “On the Principles and Guarantees of Freedom of Information”, “On Informatization”, “On Personal Data”, “On State Secrets”, “On Electronic Government”, and “On Electronic Digital Signature”. While these laws frequently complement one another, they also sometimes overlap or even contradict each other. For this reason, it is necessary to systematize the existing normative-legal framework, clarify the scope of regulation, repeal redundant or outdated provisions, and most importantly, develop a codified act—the Information Code—that would fully cover issues of information security, access to and protection of information, the safeguarding of citizens’ rights to information, and new threats arising from technological development.

Third, it is necessary to formulate a broadened definition of information security that reflects evolving social relations. This definition may be expressed as follows:

Information security is a system of legal, organizational, technical, and social measures aimed at ensuring the confidentiality, integrity, availability, and reliability of information, as well as protecting it from unauthorized interference; and at safeguarding the interests of individuals, society, and the state in the information sphere against any internal or external, accidental or intentional threats.

The comprehensiveness of this definition lies, first of all, in its reference to all qualitative characteristics of information. If any one of these elements is missing, information security cannot be considered guaranteed. Furthermore, as the analysis of existing legislation suggests, information must be truthful and complete. The adoption of this definition would provide a conceptual foundation for information security. Second, it integrates both subjective and objective interests—those of the state, society, and individuals—in a coherent manner. Third, it explicitly classifies the nature of threats as internal, external, accidental, or deliberate, which is crucial in the context of the growing complexity and diversity of digital objects. Finally, it specifies a detailed classification of protective measures.

CONCLUSION

In conclusion, while Uzbekistan’s current legislation contains a number of positive elements in ensuring information security, which continue to expand in response to evolving social relations, there remain shortcomings that must be addressed. Legislative development in this area should be pursued in a systematic and consistent manner. Importantly, foreign experience—particularly the practices of Germany, Russia, and other European states—should be carefully studied. By doing so, Uzbekistan can identify which measures have proven effective in ensuring information security and which deficiencies have hindered success.

Alongside the positive aspects, the analysis has revealed certain weaknesses, including the vulnerability of state information resources, the absence of a unified normative base, and the lack of a comprehensive and adaptable definition of information security. The solutions proposed above are intended to eliminate these deficiencies and to strengthen the national framework for information security in line with international standards.

REFERENCES

1. State Committee of the Republic of Uzbekistan on Statistics, 2025//https://stat.uz/uz/
2. Cybersecurity Ventures. (2020). Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Retrieved from: https://cybersecurityventures.com/cybercrime-

damages-2025

3. Qonun hujjatlari ma'lumotlari milliy bazasi, 06.10.2020-y., 06/20/6079/1349-son// https://lex.uz/ru/docs/-5030957
4. https://www.bmjv.de/
5. https://normativ.kontur.ru/
6. Criminal Code of Estonia, 2002, http://www.legaltext.ee/text/en/X30068K8.htm
7. https://infocom.uz/articles/ozbekistonda-kiberxavfsizlik-rivojlanish-darajasining-tahlili