Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

THE PREVENTIVE POTENTIAL OF DIGITAL CULTURE FORMATION AND INFORMATION ETHICS DEVELOPMENT

S. S. Bakhromov
PhD Candidate, Fergana State University

Abstract
This article examines the preventive potential of digital culture formation and the development of information ethics in ensuring public security and preventing cybercrime from a socio-philosophical perspective. It reveals the theoretical foundations for fostering individuals' conscious, responsible, and ethical behavior within the information environment under the conditions of rapid digital transformation. The study also highlights the interrelationship between digital culture, information ethics, and spiritual immunity, emphasizing their role as preventive mechanisms against cyber threats. Furthermore, the article presents scientific conclusions and practical recommendations aimed at creating a secure information environment through the development of digital culture, the broad implementation of information ethics principles, and the strengthening of individuals' spiritual immunity.

Keywords: Digital culture, information ethics, spiritual immunity, digital society, cybercrime prevention, information security, digital literacy, socio-philosophical analysis.

Web of Humanities: Journal of Social Science and Humanitarian Research

Introduction

In the 21st century, as a result of the deep penetration of digital technologies into all spheres of life, a new stage of social development is being formed - the digital society. Digital transformation, along with increasing the efficiency of public administration, the economy, education, medicine and social relations, also puts on the agenda new tasks such as information security, personal spirituality, the culture of information use and the formation of sustainable immunity against cyber threats.

Although the Internet and social networks have become an integral part of human life today, the disinformation, manipulative content, cyber fraud, illegal acquisition of personal data, and other information threats distributed through them negatively affect the sustainable development of society. This shows that it can be prevented not only by legal or technical means, but also by increasing the spiritual stability of the individual, the culture of working with information, and moral responsibility.

In this context, digital culture and information ethics are important social mechanisms for preventing cyber threats. While digital culture forms the skills of a person to act intelligently, responsibly and safely in the digital environment, information ethics ensures compliance with universal human values, legal norms and ethical principles in the process of creating, distributing and using information. The combination of these two factors serves to develop critical thinking, a responsible attitude and spiritual immunity in a person towards information threats.

Each civilization has its own spiritual protection system. National values, historical memory and cultural identity are important factors of spiritual immunity. In the 21st century, human development is characterized by an unprecedented increase in the speed of digital technologies,

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

artificial intelligence, global communication networks and information exchange. In such conditions, the issues of spiritual security, moral stability and cultural integrity of society have become a global problem. In particular, destructive ideas emerging in the digital space, cybercrime, manipulative information, virtual violence, the negative impact of mass culture and ideological threats directly affect the human mind. Therefore, the concepts of “spiritual immunity”, “information ethics” and “digital culture” have become one of the important categories of modern socio-philosophical research. These concepts are manifested as a preventive mechanism that ensures not only the security of the individual, but also the spiritual stability of society and the ideological security of the state. Preventiveness - that is, the function of preventing negative situations - is especially relevant in today's era of globalization and digital transformation. The term "immunity" originally meant the body's ability to protect itself against external harmful factors in biological sciences, but in a socio-philosophical context it means the ability of a person and society to provide spiritual and moral resistance to harmful ideas, moral violations, ideological threats, and destructive information. Spiritual immunity, information ethics, and digital culture are the most important preventive institutions of a modern digital society.

They are:

the spiritual security of society;

the ideological stability of young people;

the health of the information space;

plays an important role in ensuring the digital responsibility of citizens.

If spiritual immunity is an internal mechanism that protects a person from destructive ideas, information ethics determines the moral norms of digital communication, and digital culture forms conscious and responsible activity in the virtual space. Therefore, in the context of digital transformation: strengthening spiritual education; developing media literacy; integrating information ethics into the education system; popularizing cyberculture remain one of the priority strategic directions of the development of the state and society.

The rapid development of digital technologies and the expansion of the information space are creating new forms of social relations in modern society, and are also increasing the criminal risks associated with them. In particular, cybercrimes are emerging as a complex and multifactorial socio-legal phenomenon that is formed under the influence of the specific characteristics of the digital environment. A thorough analysis of the causes of the emergence and spread of these crimes is of great importance in developing effective measures to combat them and prevent them. Objective factors of emergence of cybercrimes are connected, first of all, with development of digital infrastructure, popularization of information technologies, interconnection of information systems and possibilities of anonymity in cyber environment. Such factors create technical and organizational conditions for committing crimes, lead to decrease in level of detection and ease of implementation of cybercrimes. At the same time, transnational nature of cybercrimes strengthens influence of these factors.

The subjective factors of cybercrime are determined by the individual's legal awareness, moral views, attitude to social values, material interests, and behavioral characteristics in the virtual space. In particular, the incorrect or insufficient formation of digital literacy, the weakening of the sense of responsibility in the virtual environment, and the feeling of anonymity are manifested as

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

subjective factors that encourage criminal behavior.

In this regard, a comprehensive scientific analysis of the objective and subjective factors of the emergence of cybercrimes serves as a solid theoretical basis for a deep understanding of the causes of these crimes, their classification, and the development of effective prevention and countermeasure strategies. This paragraph systematically studies the factors that cause cybercrimes, analyzes their interrelationships and the features of their manifestation in the conditions of a modern digital society.

As the current processes of globalization and digital transformation penetrate all spheres of society, the issues of information security and combating cybercrime are gaining urgent importance. The expansion of information and communication technologies, the popularization of the Internet and the proliferation of digital services create vast opportunities for society, but also create new threats. Therefore, reforms in the information sector require not only the development of infrastructure, but also ensuring cybersecurity, improving legal mechanisms and effectively combating new types of crime.

The multifaceted and rapidly changing nature of cybercrime further increases the damage it can cause to society, the economy, and state security. Personal data of citizens, state information resources, commercial secrets, and financial systems are becoming the main targets of cyberattacks. This situation requires further strengthening of cybersecurity and legal and organizational measures in the framework of reforms being implemented in the information sector. Uzbekistan is implementing consistent reforms to protect the information space, ensure the security of digital services, and combat cybercrime. The adoption of new legislation, the development of the activities of specially authorized bodies, the expansion of international cooperation, and the improvement of the public's cyber hygiene culture are important components of these efforts.

It is these factors that increase the importance of an analytical approach to this topic and indicate the need for a comprehensive study of the issues of combating cybercrime in the system of reforms in the information sector.

It is known that the rapid development of information technologies has a profound impact on all aspects of social life. The expansion of digital infrastructure, the popularization of electronic services and the widespread use of the Internet, while creating great opportunities for the development of the country, also creates new types of threats in the information sphere. In particular, crimes committed with the help of information technologies - cyberattacks, illegal acquisition of personal data, financial fraud, distribution of malicious programs and other types of offenses - pose a serious threat to the security of the state and society.

In such circumstances, it is urgent to take comprehensive measures to increase the effectiveness of the fight against cybercrime, ensure stability and security in the information space, and protect the rights and interests of citizens.

It is precisely on the above issues that the Head of State Sh.M. Mirziyoyev developed Resolution No. PQ-153 “On measures to further strengthen activities to combat crimes committed using information technologies” dated April 30, 2025. This resolution is aimed at further strengthening activities to combat crimes committed using information technologies, strengthening cooperation between authorized organizations, and improving legal, organizational and technical mechanisms to ensure cybersecurity.

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

The measures set out in the resolution serve to prevent cybercrime in the country, ensure order in the digital environment, improve citizens' information literacy, and increase the level of general information security. At the same time, these initiatives are also aimed at adhering to the principles of cyberethics, forming responsible digital behavior in society, and strengthening ethical standards in the information space.

This resolution identifies several priority areas for combating crimes committed using information technology:

1. Strengthening the legal framework and control mechanisms.

- Improving legislative documents on cybercrime.
- Adapting the standards defining the composition of a crime to modern threats.
- Digitalization of inspection, operational search and examination processes.

2. Strengthening the activities of competent authorities.

- Increase the capacity of special departments and sectors for information security.
- Implementing advanced technologies to detect and prevent cyberattacks.
- Strengthening mechanisms for interaction between government bodies, law enforcement agencies, and business entities.

3. Development of technical protection measures.

- Providing information systems with border protection, cryptographic programs, and monitoring systems.
- Develop cyber security response centers (SOCs).

4. Formation of cyberethics and digital culture.

- Promoting cyberethical behavior among the population, especially young people.
- Introduction of special programs on information culture and cyberethics in educational institutions.
- Strengthening the principles of responsible information dissemination and respect for personal data in the media space.

5. Strengthen international cooperation.

- Conducting joint research and operations against cybercrime with foreign countries.
- Information exchange and implementation of joint security standards.

The significance of this decision can be analyzed from several perspectives:

1. From a national security perspective. Attacks on information systems pose a serious threat to strategic sectors such as public administration, the banking and financial system, transport, and energy. The measures set out in the resolution will serve to ensure the stable operation of these infrastructures.

2. From the point of view of economic stability. The financial losses and security restoration costs from cyberattacks negatively impact economic growth. Reducing moral and financial losses through crime prevention increases economic efficiency.

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

3. Society and youth issues. Young people are the main users of the digital environment. If they do not develop cyberethical skills, their tendency to commit crimes increases. The decision will greatly contribute to the formation of moral responsibility, a culture of safe use, and rules for the correct handling of information among young people.

4. From a cyberethical perspective. Most crimes, such as cyberattacks, disinformation, blackmail, and personal data breaches, are related to violations of ethical rules. The resolution stipulates measures aimed at strengthening cyberethical education and ethical standards, which are an important factor in eliminating the causes of crimes.

5. Compliance with international standards. The tasks set out in the resolution are consistent with international cybersecurity norms and serve to increase the country's influence in the global digital space.

This resolution on combating crimes committed using information technologies is an important step towards building a digital society. It provides for a comprehensive approach based on cyberethics and information culture, along with legal, technical and organizational mechanisms.

Implementation of the decision:

- strengthens the security of the state and society;
- ensures stability in the information space;
- shapes ethical and responsible digital behavior in young people;
- reduces economic losses;
- strengthens national and international cooperation in the fight against cybercrime.

As a result, a safe, stable, and ethically-based digital environment will be formed in the country, and systematic work will be carried out to prevent cybercrime.

According to the law, cybersecurity entities are defined as legal entities or individual entrepreneurs that own, use and manage national information resources, as well as entities that provide electronic information services, and have certain rights and obligations related to information protection and cybersecurity. This category also includes entities of critical information infrastructure.

When discussing cybersecurity subjects in more detail, the role of the individual first of all attracts special attention. Here, an individual is an employee of a specific organization or an ordinary citizen who is responsible for complying with the established requirements and rules in the field of cybersecurity and ensuring information security. Full compliance with the established rules requires a person to have a certain level of legal knowledge and practical skills.

SocietydevelopmentAmong the current approaches to determining the place of the individual in the world, the second view - that is, the approach that focuses on the formation and development of a person through the process of socialization - is more consistent with the requirements of modern science. Because, according to modern scientific views, socialization is closely related to the growth and change of a person in the process of assimilation of culture.[1].The socialization of a person is a continuous process that continues to some extent throughout a person's life. It manifests itself in different forms and intensities at different stages of development, such as childhood, adolescence, middle age, and old age.

[1]Social pedagogy. The course is a lecture. Pod. ed. MAGalaguzovoy. -M.: VLADOS, 2003. -S. 87.

Web of Humanities: Journal of Social Science and Humanitarian Research

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

In the field of cybersecurity, reliable protection of the rights and freedoms of the individual is of great importance. Ensuring the integrity of personal data, private life and information of a person who has suffered damage as a result of a cyberattack is one of the most important tasks of cybersecurity. In this regard, first of all, ensuring the confidentiality of personal data located on the Internet and their processing only in accordance with the law is a priority task. Also, preventing the violation of a person's privacy through cyberattacks - that is, preventing the illegal acquisition or dissemination of private information - is another important area of cybersecurity.

Article 33 of the new Constitution of the Republic of Uzbekistan states that “Everyone has the right to seek, receive and disseminate any information. The state creates conditions to ensure the use of the global information network, the Internet. Restrictions on the right to seek, receive and disseminate information are permitted only in accordance with the law and only to the extent necessary to protect the constitutional order, health of the population, social morality, the rights and freedoms of other persons, ensure public safety and public order, as well as to prevent the disclosure of state secrets or other secrets protected by law.[2]"It is indicated as ".

Information and political security refers to a complex of issues related to the protection of vital interests of citizens, the state and society from internal and external information threats in the political arena. To put it more precisely, information and political security includes the following tasks: firstly, ensuring the interests of citizens, society and the state on the basis of generally accepted security standards; secondly, in connection with the rapid development of information technologies and communications, it imposes the obligation to search for and develop opportunities for effective information use against external and internal threats. As Professor John Smith noted: “Cybercrime is a killer weapon of the new era, which not only causes financial damage, but also undermines trust between people and states[3]”. Scientists argue that the concept of cybercrime includes not only the use of information technologies for illegal purposes, but also social and economic consequences. For example, T. Stoll in one of his works states: “Cybercrime not only poses a risk of loss of personal information, but also threatens the global economic balance[4]". Cybercrimes cause not only material, but also social and moral damage to society and the economy. From a scientific point of view, they lead to billions of dollars in financial losses for companies and individuals, the failure of information systems, and the illegal dissemination of personal data. This poses a serious threat to economic stability and the functional efficiency of society.

From a socio-philosophical perspective, cybercrime affects a person's sense of security, social trust, and mental stability. As a result of violations committed in the information space, psychological pressure increases among citizens, mental stress occurs, and a sense of security and trust in their actions in the digital environment and social relations decreases. This also creates a serious problem for the moral and cultural stability of society, since the responsibility of each individual in digital activities and the information culture determine the general social environment. Thus, cybercrime is seen as a global problem that threatens not only material losses, but also social and spiritual stability, and its prevention requires the integrated use of legal, technological, and ethical approaches.

[2]Constitution of the Republic of Uzbekistan. T. 2023 https://lex.uz/docs/6445145
[3] John Smith //Early Modern Letters Online
[4]Stoll, K. A. (2018). Cybercrime: problems and methods of analysis. New York: IT Press.

Volume 4, Issue 5, May 2026 ISSN (E): 2938-3803

The following measures are of particular importance in preventing cybercrime:

1. Improving security systems — providing information technology systems with effective protection tools.
2. Strengthening legal norms - improving laws and developing international cooperation in the fight against cybercrime.
3. Public awareness - increasing citizens' knowledge and skills in information security.
4. Using artificial intelligence and analytics tools — applying modern technologies to detect and analyze cyberattacks in advance.
5. International cooperation - strengthening cooperation between countries in the fight against cybercrime.

According to Dr. Elizabeth Gray, preventive measures are of great importance in preventing cybercrime. She emphasizes that in this process, every individual and organization must create a culture of information security[5].Teamwork is essential in preventing cybercrime, as effective action against this problem can only be achieved through cooperation between the public and private sectors. The following measures are important:

-Establishment of national centers in the field of information security.

-Establish effective cooperation between law enforcement agencies, Internet providers, and the banking sector.

-Increasing cybersecurity culture and information security knowledge among the public.

Conclusion

In conclusion, improving the legal framework, using modern technologies, and raising public awareness are key to effectively combating cybercrime. At the same time, cooperation between states is also important in preventing transnational cybercrime.

REFERENCES

1. Development Strategy of New Uzbekistan for 2022-2026. –Tashkent: Adolat National Legal Information Center. 2022.
2. On measures to organize scientific and practical research in the field of criminology / Resolution of the President of the Republic of Uzbekistan dated 15.01.2024 No. pq-22.
3.https://www.cybersecurityintelligence.com/europol-european-cybercrime-centre-ec3-9300.html.
4. Q. Nazarov Encyclopaedia of World Philosophy, Volume I "National Society of Philosophers of Uzbekistan", "Spirituality" Publishing House - Tashkent.: 2023.
5. https://wearesocial.com/digital-2020.
6.https://daryo.uz/k/2020/10/29/ozbekistonning-kancha-aholisi-internet-tarmogiga-connected.
7. https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda.
8. V.H. Dryomin Globalization informatsionnykh system kak factor globalizatsii prestupnosti // Information technologist ta bezpeka. - Kyiv, 2002.
9. Ruziev R.N., Salaev N.S. National and international standards for combating cybercrime. Monograph. – Tashkent.: TDUU, 2018.
10. www.statista.com.
11.https://cybermap.kaspersky.com/ru/stats/., see also: Anorboev A.U. Cybercrime: criminal-legal and criminological aspects.: (PhD) diss.12.00.08.,-Tashkent.: 2020.

[5]Miller R. T. (2021). Transnational Cybercrime: Challenges of Legal Protection. London: Cambridge Press.