THE MAIN ISSUES OF INTERNATIONAL LEGAL FRAMEWORK FOR REGULATION IN THE FIELD OF INFORMATION SECURITY

Nugmanov Nugman Abdullayevich
DSc, Professor University of World Economy and Diplomacy
54, Mustakillik Ave., Tashkent, 100007, Uzbekistan
E-mail: nugmann88@gmail.com
nnugmanov@uwed.uz
Mobile: +99893184005

Abstract: *The author examines the issues of international legal basis of regulation information security. Informatization contributes new threats to national, regional and global security, and accordingly, international information security is important component of the general concept of information security. The main components of information security are the security of the information space, the security of the information infrastructure and ensuring such properties of information as availability, integrity and confidentiality.*

Keywords: *international information security, international legal regulation of information security, international cooperation in the field of information security, security of the information space, security of the information infrastructure, information.*

The progressive development of ICT and globalization processes, together with positive processes, also include certain problems in the field of information security, in particular on the Internet. The Internet is one of the most significant and breakthrough achievements at the global level in the information sphere. In the modern world, the Internet makes it possible for individuals, society and states to exchange a wide variety of information online (in real time), including audio and video recordings. The Internet is not only a means of communication, but also a medium where people enter into various types of legal relationships [1].

The modern development of the concept of information security is linked to the global information revolution, in the process of which the number of modern information and communication technologies (ICT) and the scale of dissemination of these technologies are constantly and dynamically growing. At the same time, it is very likely that the successful results of the global information revolution will be used for destructive purposes, for example, for the purpose of interference by one State in the internal affairs of another or for other purposes contrary to generally recognized principles of international law. That is, the issues of ensuring the information security of the state are the subject not only of cooperation between states, but also of rivalry in

political, economic and other spheres. The formation of a completely new area of international counteraction to them, which concerns not only the interests of national security, but, also the global system of international security, determines the increasing role and importance of the problem of ensuring the information security [2]. Today, the problem of information security has moved from the field of technological categories to the field of social development management [3].

The UN General Assembly has adopted a series of resolutions on achievements in the field of information and telecommunications in the context of international security: Since 1998 (first resolution A/RES/53/70), these annual resolutions have laid the foundation for discussions. They recognize that ICTs can pose threats to international peace and security and call on states to cooperate, develop norms of behavior and build trust.

The Open Working Group (UN OWG) established in 2020 emerged as a more inclusive alternative to the GPE. Its final report (2021) confirmed and developed many of the GPE's norms, emphasizing the applicability of international humanitarian law and human rights in cyberspace.

The United Nations Convention against Transnational Organized Crime (Palermo Convention, 2000) also serves as a basis for cooperation in the fight against cybercrime, especially when it involves organized groups. In addition, the Organization for Economic Co-operation and Development, the International Organization for Standardization, and the International Telecommunication Union deal with issues of information security.

In 2024, the UN Convention against Cybercrime was adopted, a comprehensive legal instrument aimed at strengthening the global fight against cyberthreats and enhancing international cooperation. A central element of the Convention is the criminalization of a wide range of offenses committed using information and communications technology. The document identifies 11 categories of cybercrime, including traditional computer crimes (illegal access, data interception, interference with information systems), economic crimes (theft, fraud, forgery using ICT), crimes against children (posting sexually explicit material, harassment), as well as the non-consensual distribution of intimate images and the laundering of proceeds from cybercrime.

At the regional level, within the framework of the Council of Europe, the source of international legal regulation of various aspects of international information security is the Convention on Cybercrime (Budapest Convention, 2001). This agreement is a key international legal instrument in the fight against cybercrime. It establishes standards for national legislation, investigation procedures and mechanisms for international cooperation (extradition, mutual legal assistance). It has an Additional

Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems (2003).

Within the framework of the SCO, an Agreement on Cooperation in the Field of International Information Security was adopted (2009, entered into force in 2011). This agreement emphasizes the principles of sovereignty, non-interference, and combating the use of ICT for terrorist, extremist and criminal purposes. ASEAN, OAS.

The African Union and other international organizations are also developing regional approaches and cooperation in the field of information security and the fight against cybercrime.

What are the key issues and trends in the field of international legal regulation of international information security? Firstly, there is the problem of fragmentation, i.e. the lack of a single, comprehensive treaty. Existing norms are mainly based on 'soft law' (resolutions, reports of the GPE/OVRG) and regional instruments (the Budapest Convention).

Secondly, there are disagreements between states, as there are currently different approaches to ensuring international information security. Some countries believe that cybersecurity is primarily about protecting systems and data and regulating issues related to cybercrime. Other countries believe that ensuring international information security is primarily about preventing interference in internal affairs ('information weapons', 'color revolutions').

Thirdly, there is hyper-dynamic technological development, meaning that international law cannot keep pace with technology, especially in areas such as AI, quantum computing and the Internet of Things.

Fourthly, there is the role of non-state actors, i.e. the difficulty of controlling at the state level the growing threat posed by the international activities of criminal groups and terrorists.

It is clear that the international legal framework for information security is still being developed. It is based on the principles of the UN Charter, norms of responsible behavior by states (developed by the UN Working Group on Disarmament Matters and the UN Working Group on Disarmament Questions), regional treaties (especially the Budapest Convention) and confidence-building measures. However, key challenges – fragmentation, political disagreements between states on fundamental issues and the speed of technological change – are still hindering the creation of a unified, universal and effective system of international legal regulation of information security. Development is moving in the direction of strengthening cooperation, developing specific norms and trust, but the path to a comprehensive convention remains difficult.

Undoubtedly, cyberterrorism poses a threat of attack on so-called critical information infrastructures that allow critically important objects (or processes) to function. These include national telecommunications systems, airfields, gas pipelines,

etc. As a result of destructive impact on such infrastructures, the probability of a catastrophic situation caused by disruption of their information systems and fraught with enormous negative consequences on a national scale increases many times over [4].

The interconnectedness of digital infrastructure allows cyber threats to easily cross borders, causing widespread damage. A data breach in one country can impact international markets, highlighting the economic risks of weak cybersecurity [5]. Attacks on critical infrastructure, like energy grids and healthcare systems, pose national security risks [6]. As Cybersecurity Ventures reports, global spending on cybersecurity is expected to exceed $1.75 trillion from 2021 to 2025 [7].

It should be noted that the problem of ensuring information security is complex in nature and includes two main aspects. The first aspect concerns issues related to the content of information, namely the compliance of the information disseminated with certain standards, including generally accepted principles of international law.

The second aspect concerns issues related to various means of information processing. These means include various technical means for collecting, accumulating, storing and transmitting information, including information and telecommunications networks and computers. It should be noted that issues related to ensuring the operation of information processing tools include not only technical aspects, since ensuring information security for various government organizations includes such properties of information related to its processing as integrity, confidentiality and accessibility, and this already requires appropriate legal regulation.

The division of information security into the two aspects mentioned above reflects the need to reflect that they relate to two different spheres of public relations and are therefore regulated by different legal regimes. This understanding of the division of the concept of information security into two aspects contributes to the correct legal regulation of information security issues.

It should be noted that interstate relations in the field of information exchange are subject to the norms and principles of international law, which regulate various aspects of the dissemination of information at the international level [8].

The fundamental legal principles on which the system of legal support for information security is based must be enshrined in a single international treaty, which, firstly, will be the final stage in achieving consensual approaches between major entities of international legal relations, and secondly, will contribute to uniformity in the procedures and mechanisms for ensuring international information security. In this regard, one cannot but agree with the following statement by A.K. Duben: "the fundamental principles in the field of ensuring international information security require enshrining at the global level, since the supranational level of legal support on a regional scale, which involves the participation of several (or several dozen) states,

cannot fully satisfy the needs of the world community in solving the problems of international information security" [9].

Furthermore, it should be noted that the development of a global and secure information society is a complex process demanding continuous monitoring, analysis, and active international multilateral cooperation. Therefore, in light of the regrettably negative trends in the international information environment, it's imperative to not only promote positive developments within the international legal framework concerning information security but also to further enhance practical, compromise-driven inter-state collaboration on various aspects of international information security [10].

We agree with the opinion that in the global information society, the task of finding the necessary modern universal and complexly organized legal mechanisms for building a system of legal support for information security, taking into account the peculiarities of the transformation of law, the need for closer development of legal, technical, moral and corporate norms, as well as extrapolation of the methods of technical and natural sciences used in the study of technical regulation of information security, into the legal sphere for building a universal concept of legal regulation of ensuring information security, is especially urgent [11].

It should also be noted that the realization of citizens' fundamental rights and freedoms in the information sphere is a key issue for the national interests of any state. This is based on the principles of freedom of information and the prohibitive principle of law (everything not prohibited by law is permitted) [12].

Based on the above, it can be concluded that the main components of ensuring information security are, first, the security of the information space, which is necessary for the use of information for peaceful purposes; secondly, the security of the information infrastructure, which is necessary to prevent the negative impact of information on the system being used; and thirdly, ensuring such properties of information as accessibility, integrity and confidentiality.

References:

1. Nugmanov N. A. International legal regulation of the fight against cybercrime // German International Journal of Modern Science / Deutsche Internationale Zeitschrift für Zeitgenössische Wissenschaft. – 2023. – №. 65.
2. Nugmanov N.A. Information Security Concept Major Aspects and Specifics // International Affairs: Politics, Economics, Law. Volume number 1-2 / 2024. - P. 118-136.
3. Nugmanov N.A. International Legal Regulation of Information Security within the UN // International Affairs: Politics, Economics, Law. Volume number 9-10 / 2023. - P. 160-170.

4. Nugmanov N.A. Problems of Formation of International Standards for the Implementation of a Unified Approach to Ensuring Information Security // International Relations: Politics, Economics, Law. – T., 2016. – No. 2. – P. 65
5. Keman Huang, Stuart Madnick & Fang Zhang, Navigating Cybersecurity Risks in International Trade, HARV. BUS. REV. (Dec. 2, 2021), https://hbr.org/2021/12/navigating-cybersecurity-risks-in-international-trade.
6. Gregg Lindemulder & Matt Kosinski, What Is Cybersecurity?, IBM, https://www.ibm.com/topics/cybersecurity (Aug. 12, 2024).
7. David Braue, Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025, Cybersecurity Ventures (Sept. 10, 2021), https://cybersecurityventures.com/cybersecurity-spending-2021-2025/.
8. Нугманов Нугман Абдуллаевич. Международно-правовое регулирование сотрудничества в области международного обмена информацией // Вестник ПАГС. 2015. №2 (47). URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-sotrudnichestva-v-oblasti-mezhdunarodnogo-obmena-informatsiey. (Nugmanov N.A. International Law Regulation of Cooperation in the Sphere of International Information Exchange // Bulletin of the Volga Region Institute of Administration. Science journal №2 (47), 2015. Saratov. – P.40).
9. Gorbunov I.A. Information security: international legal aspects of its provision // International law. 2024. No. 1. P. 38.
10. Nugmanov N.A. Some issues of the regulation of international relations in the sphere of information security //Thematics Journal of Law. Vol-5-Issue-6-June-2021. – p.37.
11. Polyakova T.A. Actual problems of development of the system of legal support of information security // Bulletin of the O.E. Kutafin University (MSAL), 2019, P. 43.
12. Нугманов Н.А. Международно-правовое регулирование информационных прав человека и границы их возможного правового ограничения // European science. – 2016. – №. 11 (21). – С. 48-53.