Chapter

Legal Aspects of International Information Security

Valentina Petrovna Talimonchik

Abstract

The objective of the research is considering the international information security concept that has developed at the global and regional levels and analysis of legal instruments for its implementation and resolving problems of the regulation of relations in the global information society. A complex of general scientific and philosophical methods including the formal-logical, comparative-legal, formal-legal, systemic-structural, and problematic-theoretical methods, as well as methods of analysis and synthesis, generalization and description, and comparison, was used in the research. As a result of the research, it has been found that a unified concept of provision of the international information security has developed at the global and regional levels, which needs legal instruments for its implementation at the global level. In the drafting and acceptance of international treaties at the global level, the experience of the Council of Europe in prosecution of cybercrime and protection of privacy should be used. The findings can be used in the activities of international organizations in execution of their functions of unification and harmonization of the international information security law and by the national telecommunication operators in the process of entering international and foreign markets.

Keywords: international law, global level, regional level, information security, cyberterrorism, computer crimes, privacy

1. Introduction

The technological progress has led to radical changes in the contemporary world. The system of international relations changed. The development of information and communication technologies (ICT) has affected all the areas of public life including the economy, politics, social issues, and culture, bringing them together in the framework of establishment of an information society.

By the present time, the information society concept has been represented in a number of international documents among which are the Declaration of Principles entitled "Building the Information Society: a Global Challenge in the New Millennium" (hereinafter referred to as the 2003 Declaration) and the Plan of Action of the World Summit on the Information Society of December 12, 2003.

Information society is a more general category as compared to the global information society. It can be established within a single state or at the regional or global levels. At the global level, it will be referred to as the global information society.

The global information society can be defined as a system of international relations that are established in the sphere of operation of information systems, which

are based on information and communication technologies, in which international information relations affect political, economic, social, and cultural relations. At the same time, the states participate in relations in the global information society as equal subjects of international information relations.

The development of ICT is related to the effect on established branches and institutes of international law as well as to the regulation of new relations that arise as a result of ICT development.

The most complicated problem is the effect of ICT on established branches and institutes of international law. The mechanism for the development of international law provisions is such that legal regulations tend to "fall behind" the level of ICT development.

Currently, the spreading and use of ICT affect the interests of the entire international community; these technologies can potentially be used for purposes that are incompatible with the objectives of international stability and security and can have an adverse effect on the integrity of the infrastructure of the states, disturbing their security in the civil and military areas.

The efforts of individual states are insufficient for ensuring international information security. First of all, the prohibition on the use of information weapons by states must be established in international law. Separate regulation is required for matters of information security of individuals (protection from defamation and privacy).

The forming special principles of international information law include the principle of confidentiality and security in using ICT. Strengthening the trust framework, including information security and network security, authentication, privacy, and consumer protection, is a prerequisite for the development of the information society and for building confidence among users of ICTs. A global culture of cyber security needs to be promoted, developed, and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber security, it is important to enhance security and to ensure the protection of data and privacy while enhancing access and trade. In the 2003 Declaration, the term "cyber security" has a wider meaning that only protection from cybercrimes. In particular, the Declaration notes that the summit participants support activities of the United Nations to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within states, to the detriment of their security.

These regulations ensure the relation of the developing principle of international information law with the existing principles, namely, the principle that the exercise of freedom of opinion, expression, and information is an essential factor in strengthening peace and international security; the principle that the media should contribute to the strengthening of peace and international understanding and to the struggle against racism, apartheid, and incitement to war; and the principle of the need to publicize the denunciation of information, the spreading of which has caused damage to efforts of strengthening of peace and international understanding, the development of human rights, and the struggle against racism, apartheid, and incitement to war.

The problems of information security of individuals and legal entities have been examined in fundamental research on the comparative law of information technologies by Bainbridge [1], Campbell [2], Rowland and Macdonald [3], Smedinghoff [4], and Black [5].

The issue of privacy protection, primarily using national legal instruments, has been covered in particular chapters in the fundamental research on the law of

information technologies by Bell and Ray [6], Reed [7], and Angel [8] and special research by Solove [9] and Nouwt, Berend, and Prins [10].

Technical and organizational aspects of ensuring information security have been covered in the works of Egan and Mather [11], Hunter [12], and Volonino and Robinson [13].

The matter of implementation of the concept of ensuring international information security has already been considered in research, although the concept itself has not been stipulated. Lloyd [14] considered the acts of the UN, the Council of Europe, OECD, and the Asia-Pacific Community when addressing the issues of privacy, primarily considering "soft law" acts. In a review of cybercrime problems, this author gives a brief overview of the Council of Europe Convention on Cybercrime, the OECD Guidelines for the Security of Information Systems, and the EU acts.

The contents and significance of the Convention on Cybercrime of November 23, 2001, have been discussed in the studies by Lloyd [14], Murray [15], and Koops, Lips, Prins, and Schellekens [16]. But these studies did not cover the problems of using the experience of the Council of Europe at the global level.

With regard to the 2001 Convention, Hopkins [17] has noted its excessive broadness and lack of clarity in its basic terms. For example, this Convention defines a computer system as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. In such case, the term device will include children's toys, Palm Pilots, and cable television devices. Therefore, the scope of the 2001 Convention extends from real computer crimes to interference in any devices where software is used.

The concept of personal data in international acts has been criticized in the legal doctrine. In particular, Berčič and George [18] state that this definition is too broad because any information about a person can be regarded as personal data (e.g., information that an individual is wearing a red shirt). On the other hand, there arise practical complicacies with attributing certain data as personal data (e.g., social security identification numbers).

Polcak [19] has pointed out that in various European countries, there are complicacies with attributing IP addresses, personal telephone numbers, data entered anonymously when receiving services via the Internet, and data of deceased persons as personal data.

The absence of unified list of personal data in the national legal systems is the reason of the imperfection of the international legal regulation. The efforts made in the area of harmonization have not been successful enough. This is confirmed by the attempts that are being made at the national level to create an own definition of personal data. In particular, a number of authors have named the Durant v. FSA case in British courts as an example. In this case, the Court of Appeals has defined personal data as information that affects the privacy of the data subject including their personal and family life and business or professional abilities [20].

It should be noted that currently, proposals to make global international treaties primarily come from non-state actors. In August 2000, a group of researchers from Stanford University presented the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the Stanford Project). Brown drafted a convention regulating the use of information systems in armed conflicts. On November 6, 2009, the International Conference of Data Protection and Privacy Commissioners adopted a resolution entitled "Standards of Privacy and Personal Data," for which it established a work group to develop a draft global treaty and listed the criteria for the drafting of it. It is planned to submit the developed sections of the treaty to the UN. Thus, researchers and international forums are proposing specific projects, but no systemic work is carried out in the framework of the UN, International Telecommunication Union (ITU), or UNESCO.

At the same time, there are no monographic researches of the general concept of international information security that would cover the regional and global levels and the problems of development of its legal basis.

The present study, based on the analysis of international acts, reveals the content of the general concept of international information security that would cover the regional and global levels. "Soft law" acts are appropriate for the formulation of the general concept of international information security, but not for its implementation. Therefore, the author proposes a draft convention with the purpose of creating of global network of information security.

2. Analysis of international acts

The objective of the research is consideration of the international information security concept that has developed at the global and regional levels and formulation proposal for elaboration of legal instruments for its implementation in connection with the concept of the global information society. For this, the analysis of existing international information security system at the global and regional levels shall be made, a description and a generalization of the analysis results. For the analysis of existing international information security system, formal-logical, systemic-structural, and problematic-theoretical methods have been used. At the same time, comparative-legal method is used to analyze the provisions of information security at the global and regional levels.

In order to solve the problems of international security that have arisen with the development of ICT, the UN General Assembly has adopted resolutions entitled "Developments in the field of information and communications in the context of international security" at each of its sessions since 1998. The main idea of these resolutions is that the significant progress, which has been achieved in the development and implementation of the latest information technologies and telecommunications, has caused negative consequences as well as positive ones. At the same time, the positive consequences, namely, new opportunities for the entire mankind, are obvious.

However, the UN General Assembly has expressed concern that new technologies and facilities that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of states to the detriment of their security in both civil and military fields.

The resolutions invite states to inform the UN Secretary-General on the following issues, namely, (1) general assessment of the problems of information security, (2) development of concepts relating to information security, and (3) development of international principles aimed at ensuring information security of global information and telecommunications systems and combating information terrorism and crime.

It should be noted that there exist resolutions which confirm a certain progress in ensuring information security. They contain specific proposals for the development of an information security system that can be used for the draft of relevant international treaties. For example, the UN General Assembly adopted the Resolution No. 58/199 of December 23, 2003, on the creation of a global culture of cybersecurity and the protection of critical information structures, which defines elements for protection of critical information infrastructures, namely, (1) having emergency warning networks regarding cyber-vulnerabilities, threats, and incidents; (2) raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play

in protecting them; (3) examining infrastructures and identifying interdependencies among them, thereby enhancing the protection of such infrastructures; and (4) promoting partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures, etc.

The nature of the elements for protection of the most important information structures is such that they can be included in an international treaty if they are specified.

Currently, an institutional mechanism for ensuring international information security has been established in the framework of the UN. States submit their assessments of the condition of information security on a regular basis, which are included in the reports of the Secretary-General and have contributed to a better understanding of the essence of problems of international information security and related concepts.

The work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the resulting report (2015) have been quite effective. The Group concluded that international law and, in particular, the Charter of the United Nations are relevant and important for the maintenance of peace and stability and the development of an open, safe, stable, accessible, and peaceful information environment; that voluntary and non-binding standards, rules, and principles of responsible behavior of states in the use of information and communication technologies can mitigate the risk of violation of international peace, security, and stability; and that, subject to the unique features of the information and communication technologies, more standards can be developed over time.

In addition, the EU, OAS, and Caribbean Community (CARICOM) have achieved certain results in the development of regional concepts of the improvement of information security. For example, on February 7, 2013, the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" was adopted. The strategy contains principles for cyber security, strategic priorities, and actions. The principles of cybersecurity include the principle that the EU's core values apply as much in the digital as in the physical world; protecting fundamental rights, freedom of expression, personal data and privacy; access for all; democratic and efficient multi-stakeholder governance; and a shared responsibility to ensure security.

In order to support member states in their fight against cybercrime, OAS, through the Inter-American Committee Against Terrorism (CICTE) and the Cyber Security Program, is committed to developing and furthering the cyber security agenda in the Americas. Cooperating with a wide range of national and regional entities from the public and private sectors on both policy and technical issues, the OAS seeks to build and strengthen cyber security capacity in the member states through technical assistance and training, policy roundtables, crisis management exercises, and exchange of best practices related to information and communication technologies.

CARICOM Ministers with responsibility for information and communication technologies met on May 19, 2017, as efforts continue to move on the establishment of the CARICOM Single ICT Space. Several preparatory meetings of officials were held to advance work on the Integrated Work Plan for the Single ICT Space and the draft Terms of Reference for the CARICOM-US Joint Task Force. The Integrated Work Plan will set out the activities that need to be completed for the development of the Single ICT Space. The activities of the work plan will focus on areas such as

conducting gap analyses, public awareness, specific telecommunications issues, legal and regulatory reform for cyber security, bringing technology to the people, resource mobilization, as well as forecasting for the CARICOM Digital Agenda 2025. The Single ICT space and the Region's Digital Agenda 2025 will be constructed on the foundation of the Regional Digital Development Strategy (RDDS) which was approved in 2013 and will also have inputs from the Commission on the Economy and the Post-2015 Agenda.

The concept of international information security is developing in the framework of soft law. International treaties in this field are quite scarce.

The privacy problem has been represented in the international law. Currently, the privacy provision is contained in many international documents. Of particular importance is Article 12 of the 1948 Universal Declaration of Human Rights, which stipulates that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. States recognize noninterference in personal and family life as a fundamental human right. It should be noted that the 1948 Universal Declaration is a recommendatory act, but a number of its provisions represent the established international customs. At the same time, the right to protection of private life may be restricted, which makes it impossible to regard it as a right that is recognized unconditionally.

Currently, the protection of privacy has a treaty origin. Provisions for protection of privacy are stipulated in Article 17 of the 1966 International Covenant on Civil and Political Rights, Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, and Article 11 of the 1969 American Convention on Human Rights.

Article 12 of the 1948 Universal Declaration of Human Rights has been incorporated into Article 17 of the 1966 International Covenant on Civil and Political Rights. Everyone has the right to the protection of the law against such interference or attacks. Similar provisions are stipulated by regional international treaties.

It appears quite reasonable to abolish the unification of the concept of privacy and personal data as a component of privacy in international law. Privacy is an area where individual needs of a person to be left to himself/herself are revealed. Every individual will delineate the limits of his/her privacy to himself/herself. Contemporary international law is limited to the regulation of matters of collection, processing, storage, and transfer of personal data, which are not the only issues of privacy. It appears that the privacy provision in the International Covenant on Civil and Political Rights is quite generalized but does not require specification in the information age, as it enables any individual to protect privacy in every case when the individual so wishes.

The problem of personal data protection in the framework of information security problems is perfectly reasonable to be considered. Information security is a category applicable to all subjects of information relations including states and non-state (legal entities, individuals, TNCs, nongovernmental organizations, etc.) ones. Information security of individuals is related to the respect of their privacy in the information sphere, protection from defamation, libel, insults, psychological pressure, information terrorism, etc. Therefore, the legal problems of privacy in the information sphere are a component of legal regulation of information security of the individual.

If one tries to define the content of privacy in the information area, it will be different for every individual. In the information sphere, the range of data that a person tries to make inaccessible to the public is always different. For example, one person will not hide the fact that they are infected with HIV and may say it in

an interview to a journalist, while another person will choose to not even tell close friends about it. Thus, the boundaries of privacy are always individual.

Contemporary international law provides limited privacy protection because it cannot adapt to the needs of each individual due to the general nature of the provisions. At the same time, the current international acts do not contain a list of personal data but give a fairly wide definition of such data.

An identical approach to the definition of personal data is characteristic of the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data of September 23, 1980, and the 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. In these documents, personal data are defined as any information relating to an identified or identifiable individual. Therefore, protected data include any information about an individual that can be identified. Such a broad range of protected information makes it possible to protect personal data in the situation of changing technologies that are used to collect and process data. In particular, protected data include PIN codes, logins, passwords, etc.

Despite the quite broad definition of personal data in international documents, the concept of personal data is somewhat narrower than privacy in the information area. Based on the provision of the Universal Declaration, the concept of privacy includes not just personal but also family secrets as well as the secret of correspondence. Personal data only relate to data about identified or identifiable individual. Certain provisions are applied only to individual, information on whom is stored in a particular system. For example, the 1981 Convention stipulates that any individual has the right to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; etc.

Therefore, the right to access, correct, and destroy personal data is recognized only for the person whose data have been collected. However, family secret is a different term. For example, one may conceal data about a disease of one's child or husband or addictions of deceased relatives. In essence, while personal data relate to one person, family secret is kept in a certain family and affects its collective private interests. Disclosure of family secret can harm both individual and the family as a whole including family breakdown and ruined relationships.

The existing special international acts that protect personal data in the course of their automated processing contribute to protection of not just personal but also family secrets. However, they offer no direct protection of family secrets.

As for the confidentiality of correspondence, certain provisions for telecommunications are contained in the Convention of the International Telecommunication Union. Article 40 of the ITU Convention provides for the secrecy of telecommunication messages. Government telegrams and service telegrams may be expressed in secret language in all relations. Private telegrams in secret language may be admitted between all Member States with the exception of those which have previously notified, through the Secretary-General, that they do not admit this language for that category of correspondence. Member States which do not admit private telegrams in secret language originating in or destined for their own territory must let them pass in transit, except the Constitution. ITU does not have the power to regulate information on the Internet including measures for ensuring its confidentiality. At the regional level, a provision on the confidentiality of electronic

communications is stipulated at the EU. The relevant provision is contained in the Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The most progressive in privacy protection is the EU experience. This integration organization has adopted the Regulation No. 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC (the General Data Protection Regulation) of April 27, 2016. This act is of direct effect and application in the EU Member States. A feature of the General Regulation is that any processing of personal data in the context of the activity of establishing a controller or data processing entity in the Union must be performed in accordance with the Regulation regardless of whether the data processing is affected within the Union. In order to ensure that individuals are not deprived of the protection provided by the Regulation, processing of personal data of data subjects located in the Union by a controller or data processing entity that have not been established in the Union must be governed by this Regulation if the data processing relates to the supply of goods or services to such data subjects regardless of payment. The Regulation establishes a certain legal regime for personal data processing including the conditions for their processing and requirements to their storage and transfer. The processing of personal data by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communication networks and services, and providers of security technologies and services is a legitimate interest of the relevant data controller to the extent that it is necessary and adequate as compared to the objectives of providing network and information security, i.e., the ability of the network or information system to resist (with a given level of confidence) accidental events and illegal or intentional acts that compromise the availability, authenticity, integrity, and confidentiality of stored or transferred personal data as well as the safety of the relevant services transferred via such networks and systems. Protection of privacy within the EU is also supported by the EU Court. In the Maximillian Schrems v. Data Protection Commissioner case (complaint No. C362/14), the transfer of personal data by Facebook in the USA was appealed against in the framework of the Principles of Privacy program. The EU Court concluded that the Commission had not stated in its Resolution that the USA had actually provided an adequate level of protection by virtue of their laws or international obligations. Therefore, without having to examine the content of the Principles of Privacy, Resolution 2000/520 did not comply with the EU acts in the field of privacy and is therefore invalid.

However, the EU experience takes account of the patterns of functioning of integration organizations and requires significant adaptation for use at the global level.

At the regional level, two conventions have been adopted where computer crimes are regarded as crimes of international nature. These are the Convention on Cybercrime of November 23, 2001 (hereinafter referred to as the 2001 Convention) and the Commonwealth of Independent States Agreement on Cooperation in Combating Offenses related to Computer Information of June 1, 2001 (hereinafter referred to as the CIS Agreement).

The basic ideas of these conventions are the definition of unified elements of computer crimes, which the states should include in their national law, and development of measures for combating such crimes.

The CIS agreement has no definition of a computer system whatsoever, which results in an uncertainty with regard to the object of infringement.

Both the 2001 Convention and the CIS Agreement contain definitions of computer data. However, the definition in the Agreement is more concise; namely, it is

information stored in computer memory, on machine or other device, in a form that is accessible to perception or transfer via communication channels. This definition is incomplete.

The 2001 Convention offers a broader concept; namely, computer data includes any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. As a result, the CIS Agreement does not cover any software that is inaccessible to human perception but causes computer systems to operate. Interference in such software is dangerous for the public. In this case, the broader approach in the 2001 Convention should be considered justified.

The CIS Agreement contains an attempt to define computer crime, which cannot be regarded as successful. A crime in the field of computer information is described as a criminal offense, the object of infringement in which is computer information. This definition is different from the definition that has been accepted in the doctrine. It is not mentioned that computer information can be both the object and the means of an offense.

The 2001 Convention contains a number of terms that are unknown to the CIS Agreement, namely, *service provider* and *data flows*. The need to use these terms is due to the fact that the 2001 Convention defines a broader range of measures for combating computer crime than the CIS Agreement.

As for standardized elements of computer crimes, they are different in the 2001 Convention and the CIS Agreement. Some crimes have the same title but different meanings. For example, the 2001 Convention and the CIS Agreement state that illegal access to information is a criminal offense. However, the CIS Agreement is very laconic. It regards illegal access to information that is protected by law as a criminal offense if such act has caused destruction, blocking, modification or copying of information, or disruption of the operation of computers, computer systems, or their networks. The 2001 Convention stipulates that illegal access to a computer system as a whole or a part of it is a crime by itself, without stating any extra qualifying features. Therefore, the 2001 Convention prosecutes any illegal access to computer systems, while the CIS Agreement is limited to access that has led to certain consequences.

The 2001 Convention includes a number of crimes that are not covered by the CIS Agreement. These are illegal data interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, and crimes related to child pornography. A special feature of the 2001 Convention is that it covers certain common crimes (forgery, fraud) which become much more dangerous because they are committed using computers.

Therefore, the CIS Agreement uses a narrower approach to the concept of computer crime. These are only the crimes that infringe on the security of computer systems, i.e., the protected object is computer systems as such. The 2001 Convention criminalizes a broader range of acts where computer systems can be the object of or the means for committing the offense. The approach to the definition of computer crime in the 2001 Convention is more correct.

The existing contradictions in the content of international treaties on combating computer crime may result in difficulties for the states that are parties to both treaties. Basically, the provisions of the two treaties are mutually exclusive, which complicates their simultaneous application.

It should be noted that the 2001 Convention contains references to a number of international treaties. The issues of the relationship between the 2001 Convention and the CIS Agreement shall be resolved with consideration of clause 2 of Article 39 of the 2001 Convention. If two or more parties have already concluded an agreement or treaty on the matters dealt within this Convention or have otherwise

established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where parties establish their relations in respect of the matters dealt within the Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

Therefore, in the case if a state is a party to both of the abovementioned international treaties, the CIS Agreement will apply to the same matter.

Article 13 of the CIS Agreement stipulates that this agreement does not affect the rights and obligations of the parties arising out of other international treaties to which they are parties. Therefore, it allows the application of the 2001 Convention.

The existence of various regulations regarding their correlation in the considered international treaties suggests that their practical application may be complicated. For example, the states may experience difficulties in choosing the legal aid procedure. Such issues should be resolved by consultations between the states concerned.

However, in view of the harmonization nature of international treaties and the fact that the content of the 2001 Convention is broader, in the case if a state is a party to the two treaties at the same time, such state shall implement the 2001 Convention and, in the part where the provisions of the treaties are different, the CIS Agreement, as this is allowed by the 2001 Convention itself.

3. Proposal for global network of information security

The concept of developing a comprehensive system of international security is useful because of its systemic nature. This concept is not limited to military security issues but also covers economic, political, humanitarian, and information security. It should be noted that this concept needs to be clarified. Since it concerns the development of a comprehensive system of international security, it should cover the entire system of international relations. The concept of developing a comprehensive system of international security also applies to non-state international relations.

A comprehensive system of international security means a status where the interstate system is protected from the dangers that exist in contemporary world. It implies stable functioning of the system of international relations. Relations between subjects of the interstate system also include information relations. The system of such relations includes interstate and non-state relations.

Information security should be considered in two aspects.

If the systemic approach is applied, information security will act as a backbone element. It can be regarded as a status of the international relation system, which is described by stability and security from information weapons and threats.

In addition, information security can be regarded as an ideal model. There are conceptual ideas what exactly information security should be like. It is regarded in the sociological (as a certain state of social relations), technical (compliance with standards and other technical requirements), and legal (compliance with prohibitions and restrictions on the spreading of data) aspects. Based on conceptual ideas, information security can be defined as a model for stable functioning of the information relation system.

The comprehensive system of international security and information security has a certain sphere of intersection. Information security of the international system is a component of the comprehensive system of international security. However, international relations are more than just relations between subjects of international public law. The requirement of information security is equally applicable to international non-state and domestic relations.

When one uses the concept of international information security, one may define this concept based on the more general concept of information security. If one distinguishes between domestic and international information security, the first one relates to domestic information relations and the second one, to international information relations. In each of the systems of relations, information security has common features; namely, it serves as a backbone element and ensures a stable state of the system of information relations. Therefore, international information security is a status of the international information relation system, which is described by stability and security from information weapons and threats.

The development of the concept of international information security has led to the appearance of terms in the legal doctrine that had not previously been known in the practice of states. Currently, researchers use terms such as information weapons, information terrorism or cyberterrorism, and information crime or cybercrime.

The state of international legal regulation is such that these new terms have not been stipulated in treaties (save for computer crimes). However, a number of social phenomena evidence that these terms should be regarded as destabilizing factors for the system of international relations.

As for information weapons, they can be described quite generally as any means of affecting the mass and individual consciousness, which can damage, distort, destroy, or conceal data. A special feature of information weapons is that they are not used in the military field alone. Information weapons can be used for committing computer crimes, hacker attacks causing property damage, etc. The use of information weapons has been known in international practice since the second half of the twentieth century. For example, it was used widely in the Palestinian-Israeli conflict.

With the adoption of individual conventions on cybercrime, there appeared a trend in international law to prosecute the consequences of the use of information weapons rather than the weapons as such.

It should be noted that the use of information weapons has various scales. For example, information terrorism can be regarded as one of the most dangerous use of information weapons.

Information terrorism can be defined as using information weapons for undermining the constitutional order of other states or the international legal order and international relations in general.

Cyberterrorism comprises both direct terrorist activities with the use of computers, networks and data in networks, and various supplementary operations including coordination, preparation, and organization of terrorist activities using networks and data in networks and spreading knowledge about terrorism and terrorists' skills.

Individual examples of cyberterrorism have been known from the second half of the twentieth century. In 1985, a radical leftist group in Japan attacked the united railway management network using computer systems. Fortunately, the computers of the railway had good protection, which could not be hacked.

The 2001 Convention takes no account of the special features of cyberterrorism. It only takes account of "ordinary" crimes.

In this paper, computer crime is understood in the broad sense as any crime committed by using computer networks, software, or individual computers.

However, in the international law, the term *computer crime* will always have a special meaning, which is not necessarily the same as the meaning of this term in the national law. Some crimes that are punishable under the laws of one state do not affect the interests of another state or the international community as a whole.

While international crimes are threatening for the international peace and security, crimes of an international nature are common crimes in combating which states cooperate.

International crimes can be committed using computers. Global computer networks enable propaganda of war, genocide, apartheid, and racial discrimination. Moreover, the use of computers for military technology can lead to electronic communications becoming a means of aggression.

It should be noted that the existing international treaties on computer crime regard computer crimes primarily as crimes of an international nature. They define the elements of crimes that must be criminalized in national law as well as measures of international cooperation in combating such crimes.

The development of legal foundations of the global information society is to a great extent spontaneous. In the framework of the institutional mechanism of cooperation between states, there is not enough systemic vision of what the legal regulation should be like to meet the development of the technological progress.

Therefore, the information society concept needs a corresponding integral concept of international legal regulation of information exchange relations in the information society.

Some objectives have existed for a long time and are related to a lack of regulation of certain problems (matters of combating computer crime, protection of privacy at the global level, etc.), while others have appeared relatively recently as a result of technological progress.

What are the objectives that should be addressed at the global level? When determining the range of objectives, one should consider that information technologies have become global and reveal the interdependence of the contemporary world. At the same time, there is the experience of regulation of electronic data exchange relations in the framework of the Council of Europe, which should be recognized as progressive and useful for the global level.

The primary objective for the global level is solving the problems that have already been solved in the framework of the Council of Europe (combating computer crime, protection of personal data). The models of the Council of Europe have already been tested in practice, and in any case they have no significant alternative.

For the prosecution of computer crimes and protection of privacy, the global network of international information security can be created under the Security Council of UN decision by adoption of the international treaty. The global network of international information security shall provide for search in computer networks performed in one state on request of another state, real-time collection of traffic data and real-time collection and interception of content data. Therefore, the general mechanism of legal aid shall be applied, but its content is special.

In the global network of international information security, any state may request another state to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other state.

The global network of international information security stipulates 24–7 access, i.e., each state shall designate a contacting board available on a 24-hour, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data or for the collection of evidence in electronic form of a criminal offense. Basically, this procedure can take a few minutes.

The global network of international information security can also provide the access for non-state actors in privacy violations and defamation cases.

One state may get access to publicly available computer data, regardless of their geographical location, without permission of any other state. This primarily applies to data that are contained on the Internet. If a website has no access codes and the data on it can be accessible to everyone, it can be used by search, investigative,

and judicial authorities. It is a general practice of access to data in open computer networks. There exists an international custom, according to which states do not put special restrictions on the spreading of publicly available data in computer networks. Special regulations are established for data, the spreading of which is prohibited or restricted. If any person may have access to information, it would be illogical to deny such access to law enforcement authorities.

In addition, any state can access, through a computer system in its territory, stored computer data, if the state obtains the lawful and voluntary consent of the person or legal entity who has the lawful authority to disclose the data. In this case, the state body of one state must address the provider, which is located in another state, directly.

Therefore, the development of the institute of mutual legal assistance in criminal matters, which is affected by the struggle with computer crimes, is not just about introducing electronic communication technologies in traditional types of legal assistance and not just about specifying legal aid measures in relation to electronic communication technologies but also about radical change in the very content of this institute.

The system of international information security is establishing at the moment. The international information security of the interstate system is a component of the comprehensive system of international security. At the same time, international information security is a stabilizing factor in the system of non-state international relations. However, a number of threats to international information security affect the field of both interstate and international non-state relations. In "soft law" acts, a unified concept of the development of a system of international information security has been elaborated at the global and regional levels. However, "soft law" acts are not suitable for its implementation. They can contribute to development of international customs, but that can take a considerable time. Therefore, global international treaties should be drafted.

The 2001 Convention and the CIS Agreement have become the first international treaties that stipulate a system of measures for combating a specific type of crime in the field of information, namely, computer crimes. Formerly, information crimes had been covered in particular international treaties along with other crimes (such as propaganda of racial discrimination). The treaties considered have a very important role, as they have established the foundations of the jurisdiction of states for criminal cases on the Internet and the rules of international cooperation that ensure coordinated actions of states in combating computer crimes. Despite some shortcomings of the treaties, as a whole they provide for systems of interrelated international and national measures for combating computer crimes and can be the basis for drafting of a global international treaty.

IntechOpen

Author details

Valentina Petrovna Talimonchik
Saint Petersburg State University, Russia

*Address all correspondence to: talim2008@yandex.ru

References

[1] Bainbridge DI. Introduction to Information Technology Law. Edinburg: Pearson Education Limited; 2008

[2] Campbell D, Ban C, editors. Legal Issues in the Global Information Society. New York: Oceana Publications Inc; 2005

[3] Rowland D, Macdonald E. Information Technology Law. Abingdon: Cavendish Publishing Ltd; 2005

[4] Smedinghoff TJ, editor. Online Law. New York: Pearson Education Corporation; 2000

[5] Black SK. Telecommunications Law in the Internet Age. San Francisco: Morgan Kaufmann Publishers; 2002

[6] Bell R, Ray NEU. Electronic Communications Law. Richmond: Richmond Law and Tax Ltd; 2004

[7] Reed C. Internet Law: Text and Materials. Cambridge: Cambridge University Press; 2005

[8] Reed C, Angel J, editors. Computer Law: Law and Regulation of Information Technology. Oxford: Oxford University Press; 2007

[9] Solove DJ. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press; 2004

[10] Nouwt S, Berend R. In: Prins V, editor. Reasonable Expectations of Privacy? The Hague: ITeR; 2005

[11] Egan M, Mather T. The Executive Guide to Information Security: Threats, Challenges and Solutions. Indianapolis: Addison-Wesley; 2005

[12] Hunter J. An Information Security Handbook. London: Springer Verlag London Limited; 2001

[13] Volonino L, Robinson SR. Principles and Practice of Information Security. Upper Suddle River: Pearson Education Inc; 2004

[14] Lloyd IJ. Information Technology Law. Oxford: Oxford University Press; 2008

[15] Murray A. Information Technology Law: Law and Society. Oxford: Oxford university press; 2010

[16] Koops BJ, Lips M, Prins C, Schellekens M. Starting Points for ICT Regulation. The Hague: T.M.C. Asser Press; 2006

[17] Hopkins S. The Cybercrime Convention Does Not Provide Substantive Lawmaking Guidance. 2018. Available from: http://www.netdialogue.org/discussion/?p=23 [Accessed: 12 March 2018]

[18] Berčič B, George C. Identifying personal data using relational database design principles. International Journal of Law and Information Technology 2009. V. 17. N 3. P. 234-235

[19] Polcak R. Aims, methods and achievements in European data protection. International Review of Law, Computers & Technology. 2009. V. 23. N 3. P. 183

[20] McCullagh K. Protecting "privacy" through control of "personal" data processing: A flawed approach. International Review of Law, Computers & Technology. 2009. V. 23. N 1-2