

Discrepancies and Unification of the Legislation in the Field of Cybercrime

Sobirov Shokhrukhbek Tavakkal ugli

Leading Researcher of the Legislation and parliament research institute under the Oliy Majlis of the Republic of Uzbekistan

Annotation

This article examines the role of national legislation in preventing and countering cybercrime. Although there has been significant activity in the adoption of multilateral documents aimed at countering cybercrime over the past decade, this article draws attention to the increasing fragmentation of legislation at the national level.

Key words: *cybercrimes, cyber criminality, unification, legal families.*

In the context of modern globalization, law includes a large number of national, regional and international legal systems. These systems interact with each other at different levels. As a result, the rules of law sometimes either contradict each other, which leads to legal conflicts, or are not sufficiently intersected, which leads to the formation of gaps in jurisdiction¹.

Although criminal law remains the most significant instrument in countering cybercrime, we should not underestimate the norms of civil and administrative law. For example, in a number of articles of the criminal code of the CIS countries there are references to the basic requirements of administrative, civil or information law. Thus, combined approach of

different branches of law will serve as a single mechanism for preventing and countering cybercrime.

It should be noted, that almost all revealed cybercrimes contain a "transnational element". This type of crime is not the first one that requires the use of different jurisdictions and laws, but the interaction of various national, regional and international legal systems often leads to conflict of law rules, which in turn prevents the conviction of the criminal². For example, a citizen of the state of Oceania uploaded to the server in his country legitimate materials containing elements of propaganda for violence. This material was downloaded in a European country. When this citizen subsequently traveled to this European country, he

¹ Sieber, U., 2010. Legal Order in a Global World. In: Von Bogdandy, A., Wolfrum, R. (eds.) Max Planck Yearbook of United Nations Law, 14:1-49.

² Sieber, U., 2008. Mastering Complexity in the Global Cyberspace. In: Delmas-Marty, M., Pieth, M., and Sieber, U. (eds.) Les chemins de l'harmonization pénale. Paris, pp.127-202 (192-197).

was arrested and sentenced to imprisonment for this deed, which in his home country would not be considered a criminal offense.

They filed an appeal in this case. The Federal Supreme Court of this European country left the decision of the court in force, arguing that although the accused acted outside the European country, and did not actively send data directly to this country, but still created a threat to public peace in its territory in accordance with a certain rule of law. However, the court stressed that such an interpretation cannot be generalized to other norms concerning illegal content³.

From the example given, it is clear that the legal jurisdiction of one country can be activated in milliseconds. Computer data can be stored in the server of one state possibly due to lack of legal restrictions, downloaded via the Internet in many countries, in some of which this content is included into the register of malicious information, and is considered illegal.

Such examples clearly illustrate the growing discrepancy between the laws of different countries in the field of cybercrime. Some discrepancies can be explained by the fundamental differences between legal families. These include continental law, common law (Anglo-Saxon law), Islamic law and related law.

Continental criminal law is characterized by strict codification of crimes that are systematically

structured and abstracted. In addition, the Criminal Code of Continental Law contains general provisions applicable to all forms of criminal offenses⁴. Common law is the opposite of continental law. It is preceded by case law, created on the basis of a long time practice, which is considered the main source of substantive law⁵. But in all countries of common law, codified acts are being enacted in the form of separate laws, and not in the form of a criminal code. A related law was generated as a result of the impact of various legal systems, i.e. there are elements of both continental and common law⁶. Islamic law is based on Sharia and Fiqh (traditional Islamic law). Crimes are classified according to the source of the law and the prescribed punishment (hudud)⁷. In case this type of crime is not prescribed, Islamic jurists, based on Izhma and Kiyas, issue legal opinions about the public danger of this act. As we can see, Islamic law is more flexible in matters of criminalization.

Nevertheless, the difference between the general provisions of criminal law is largely explained by

⁴ Weigend, T. 2011. In: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press, pp.256 et seq.

⁵ Robinson, P. (United States) 2011, p.564. Both in: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press.

⁶ Luo, W., 2011. In: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.138; и Bu, Y., 2009. *Einführung in das Recht Chinas*. Munich: C.H. Beck, p. 20.

⁷ Tellenbach, S., 2011. In: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.321.

³ Bundesgerichtshof 1.12.2000 y (1 StR 184/00, CM. BGH MMR 2001, c. 228)

the socio-cultural and constitutional system. Because different values of the society such as human rights or the dominance of public (state) interests often have some influence in the development of strategic approaches to criminalization⁸. For example, when criminalizing such compounds as defamation or defamation on the Internet, it is extremely difficult to maintain a balance between freedom of speech and an unacceptable expression of notions.

Of course, existence of solutions to reduce the extent of discrepancies in legislation is clear. To this end, there are two approaches – either ratification and implementation of the norms of international/ regional documents or adaptation of the Country A's legislation in the field of cybersecurity and counteracting cybercrime to the legislation of Country B. These unification methods are currently actively used by many countries at the regional level, which again reduces the degree of coherence of various procedural rules with regard to international cooperation. For example, the level of coherence is higher in the countries of Europe and America than in the countries of Asia, Africa and Oceania. This can be explained by the use of multilateral legal documents in some regions, which, by their nature, are called upon to assist in ensuring coherence. At the same time, the high perceived level of

coherence of the national legislation of European countries in the field of countering cybercrime with the norms of regional documents does not fully ensure highest level of coherence of legislation within the region. These and other factors mentioned above ensure the formation of safe havens, which ensure the avoidance of criminal liability for the crime committed.

Taking into consideration the cross-border nature of a cybercrime, a subject, while on the territory of State A, can commit hacker attacks on computers of the State B. In this case, State B cannot independently carry out the necessary investigative actions that require a certain bureaucratic process, even if the Criminal Code of State A. Considering the need to protect individuals within their jurisdiction directly provides this type of crime, State A does not agree to cooperate.

Based on the above mentioned, the legislation of foreign countries provides a wide range of laws and regulations in the field of cybercrime. In particular, the criminal code, the law on the protection of personal data, the law on high-tech crimes, the criminal procedure code, the law on digital (electronic) evidence, the law on electronic operations, the law on cybersecurity and the law on international cooperation. Considering that these acts are adopted within the framework of national law, they create certain barriers to international cooperation in countering cybercrime.

⁸ Ferrante, M., 2011. In: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.13.

Thus, the complexity of national approaches can be seen in the following:

- discrepancy of legislation between legal families;

- various constitutional system and socio-cultural values of society.

The only reasonable solution is the unification of legislation in the field of cybercrime, with a view to elimination of "safe havens" for persons who committed cybercrimes. Unification of the legislation should be aimed at:

- criminalization of certain acts;
- authority of law enforcement agencies;

- issues of criminal jurisdiction;

- use of digital evidence;

- data protection;

- the responsibility of service providers;

- forms and mechanisms of international cooperation.

National approaches face a number of problems. With regard to traditional crimes, the decision of one or several countries to prosecute certain acts in court may affect the possibility of committing crimes in these countries. However, when it comes to Internet-related crimes, the ability of one country to influence a criminal is much less, since the criminal as a whole can act from anywhere where there is a connection to the network. If they operate from a country in which certain acts are not prosecuted, then international investigations, as well as requests for extradition, will often be unsuccessful. One of the main objectives of international legislative approaches is to prevent the creation of such security zones by promotion and application of world standards. As a result, national approaches in general, require additional measures that should work.