Ube International legal cooperation of the Prosecutor General's Office of the Republic of Belarus in the fight against cybercrime and typical examples of committing such crimes[1]

Andrey Hursevich[2]

ABSTRACT

The article provides the information regarding the competence and the treaty base of the Prosecutor General's Office of Republic of Belarus in a sphere of international legal cooperation on cybercrime; examines the types of crimes committed using the Internet and computer equipment, from which citizens of the Republic of Belarus most often suffer.

Keywords: *Budapest convention. Cybercrime. Internet. Mutual legal assistance. Prosecutor General's Office of the Republic of Belarus.*

1 INTRODUCTION

Currently, the Republic of Belarus is experiencing a steady upward trend in crimes committed using the Internet and computer technology, which includes the spread of malicious viruses via Internet, password cracking, theft of bank card details, phishing, drug trafficking, the dissemination of pornographic materials and materials inciting

1 Data de Recebimento: 02/09/2019. Data de Aceite: 20/09/2019.
2 Senior Prosecutor, International Legal Department, Prosecutor General's Office of the Republic of Belarus, e-mail: andr84h@gmail.com

interethnic strife and inter-religious hostility, malicious interference through computer networks in the operation of various systems and so on.

Crimes of this category are transnational in nature, that is, criminals operate in one state, and their victims are in another state. In this regard, international cooperation is of particular importance for the investigation of such crimes.

The Prosecutor General's Office of the Republic of Belarus, being one of the central competent authorities in the provision of mutual legal assistance in criminal matters, makes its contribution to the fight against cybercrime by making decisions on sending to the competent authorities of foreign states requests of Belarusian law enforcement agencies to conduct investigative and other procedural actions on their territory, as well as on the execution of the relevant requests of law enforcement agencies of foreign countries coming to address of the Belarusian side.

2 DEVELOPMENT

International cooperation of the Prosecutor General's Office of the Republic of Belarus in the provision of legal assistance in criminal cases in a sphere of cyberspace is based on existing international treaties, and in case of their absence, on the basis of the principle of reciprocity.

The treaty base of the Republic of Belarus in the field of mutual legal assistance consists of bilateral treaties, concluded with Bulgaria, Poland, Lithuania, Latvia, the Czech Republic, Slovakia, Hungary, India, China, Vietnam, Cuba, Syria, Turkey, the United Arab Emirates, Cyprus, Egypt and some other countries.

On the territory of the Commonwealth of Independent States, to which the Republic of Belarus is a party, the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Cases,

signed on January 22, 1993 in Minsk (Belarus), and the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Cases, signed on October 7, 2002 in Chisinau (Moldova), are applied as a legal instrument in this area of legal relations. The Minsk and Chisinau conventions are widely used by the Prosecutor General's Office of the Republic of Belarus as a tool to send requests for international legal assistance in criminal matters to Azerbaijan, Armenia, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine. As the name of the Minsk and Chisinau conventions itself shows, the subject of their legal regulation is widespread and concerns not only issues of assistance in the fight against cybercrimes.

In addition, the Republic of Belarus is a state party to the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of December 12, 1988, the International Convention for the Suppression of the Financing of Terrorism of December 9, 1999, the UN Convention against Transnational Organized Crime of November 15, 2000, UN Convention against Corruption of October 31, 2003, and the Council of Europe Criminal Law Convention on Corruption of January 27, 1999. These conventions may also be the legal basis for mutual legal assistance, when there is no agreement on mutual legal assistance.

As regards specialized international treaties in the field of combating cybercrime, we should mention the Council of Europe Convention on Cybercrime, signed on November 23, 2001 in Budapest (Hungary), and Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, signed on January 28, 2003 in Strasbourg (France). Despite the fact that the Budapest convention and the protocol supplementing it were prepared within the framework of a European regional political association, other countries outside the Council of Europe, including the states of the Americas, Austra-

lia, Africa and Asia, are parties to these agreements. Unfortunately, the Republic of Belarus is not a party to these international agreements, but it makes efforts to join the indicated legal instruments. In particular, representatives of the Prosecutor General's Office of the Republic of Belarus take an active part in the regional project of the Council of Europe and the European Union "CyberEast" in the countries of the "Eastern Partnership". Its working body is the Cybercrime Program Office of the Council of Europe Directorate General for Human Rights and the Rule of Law. This project aims to harmonize the national laws of the participating countries with the provisions of the Budapest convention and its supplementing protocol, increase the effectiveness of international legal cooperation between information service providers, judicial and law enforcement agencies in the field of criminal justice, the fight against cybercrime and the collection of electronic evidence. It also facilitates the exchange of experience in the fight against cybercrime between prosecutors of the Prosecutor General's Office of the Republic of Belarus, foreign experts and colleagues from the justice institutions and law enforcement agencies of Armenia, Azerbaijan, Georgia, Moldova, Ukraine and other countries.

Now let's take a closer look at some of the types of crimes committed using the Internet and computer equipment, from which citizens of the Republic of Belarus most often suffer.

One of the most common crimes committed using the Internet is the theft of money through unauthorized access to computer information.

The vast majority of requests for legal assistance issued by Belarusian investigators and received by the Prosecutor General's Office of the Republic of Belarus relate to cases of theft of money of Belarusian citizens who are registered on the Russian social networks "Odnoklassniki" and "VKontakte", which are similar to "Facebook", and are very popular in Russian Internet segment. Hundreds of these requests the Prosecutor General's Office of the Republic of Belarus sends for

the execution to the competent authorities of the Russian Federation.

A typical scheme for the commission of such crimes is as follows. The offender breaks into the account holder's profile, and then on his/her behalf begins to send messages to his/her relatives and acquaintances who are in the status of "Friends" with requests to provide details of their bank cards for depositing funds due to the loss or expiration of their own card or transfer funds to the bank account/card indicated by the offender to repay the loan, pay a fine or due to loss/theft of money during a vacation abroad.

Many Belarusians who receive such messages don't make sure that they are dealing with the real owner of the social account. They transmit the requested data or transfer money to the intruder, forgetting that the specified information is strictly confidential. As for the bank card details, having taken possession of them, the offender writes off the funds on the owner's card and transfers them to other bank accounts using various electronic payment and financial systems, including the "Qiwi", "WebMoney" and "Yandex.Money" services. Subsequently, the stolen money cashed by an attacker.

The investigation of such crimes is often complicated by the fact that criminals seek to hide traces of criminal activity, acting from abroad, indicating fictional personal data when registering electronic mailboxes and electronic wallets, using SIM cards registered to unauthorized persons, using various proxy systems servers that allow you to establish an anonymous network connection, and so on.

In order to avoid possible troubles, it is recommended to be wary of such messages coming from the aforementioned social networks, and before satisfying such requests, personally verify that they are really written by people you know.

Also in the Republic of Belarus computer fraud is quite common. In this case, the offender finds a gullible person on the Internet and, by deceiving or abusing his/her trust, takes possession of the money belonging to the victim.

A case in point is when a Belarusian woman met via "Skype" with a man who introduced himself as a citizen of the United States of America, serving in the Islamic Republic of Afghanistan in the United Nations Armed Forces. During electronic correspondence, the offender managed to gain confidence in the victim and, under the pretext of paying the costs of his arrival in Belarus for a direct meeting, took possession of the victim's funds for a total of more than $ 9,500. The victim transferred money through the "Western Union" system to foreign bank accounts indicated by the fraudster. It should be noted that the offender was very inventive in his requests for money. He provided the victim with false documents about the need to pay for vacation, air tickets and insurance, allegedly issued by the leadership of the United Nations Armed Forces. Each time, the offender found more and more circumstances hindering the meeting, to eliminate which a gullible woman had to transfer money to him. After the victim spent all her savings, including money received as a loan from the bank, and could no longer fulfill the requests of the attacker, he stopped contacting her. Of course, he didn't arrive in Belarus. As a result, the money was not returned to the deceived woman, and she is now forced to pay bank loans.

One more example. An unidentified person using the Internet, not having the intention to fulfill his obligations, posted an advertisement on the sale of women's clothing on the social network «Instagram.» Using mobile banking, the victim transferred money for the goods from her bank account to the foreign bank account indicated by the fraudster. After that, the offender stopped responding to the victim's messages, did not send the purchased goods to her and did not return the money.

In a criminal environment, computer tools are used, "inter alia", for the illicit trafficking of narcotic drugs and psychotropic substances on the territory of the Republic of Belarus.

There is a known case when criminals used online stores and

public forums of web resources for advertising and selling of smoking mixtures, spice and other drugs through bookmarks in secret places on the Belarusian territory. In order to conspire, the drug dealers used instant messaging programs with the encryption function of incoming and outgoing traffic like "Skype", "ICQ", "VIPole", "Brosix", "Jabber" and "TOR browser" to communicate with each other and with consumers. They also used "OpenVPN" software and technologies for connecting to websites through the Virtual Private Network proxy server, which ensured anonymity and changes IP address. The criminals received payment for the sold narcotic drugs and psychotropic substances by transfering money to the e-wallets "EasyPay", "WebMoney", "Qiwi" and "Bitcoin" registered to other persons controlled by them. However, the identities of the perpetrators were identified and they received a well-deserved punishment in the form of long sentences of imprisonment. In this case, the principle of inevitability of criminal liability was fully implemented.

Of particular danger is the use of a global computer network for the incitement of minors to suicide and the commission of sexual crimes against them. The following examples are indicative.

A teenage girl who is a Belarusian citizen, while on the Russian social network "VKontakte", joined the so-called "death group", similar to the groups "Blue Whale", "Quiet House", "F57". Initially, the teenager was simply interested in the reasons why people commit suicide. From the administrators of this closed group, she began to receive messages with various kinds of tasks that aroused her determination to take her own life, which she was supposed to carry out mainly at night, usually under the threat of exclusion from the group. She confirmed the fact of completing the tasks by sending photo images to the group administrators via Internet. The last thing a minor had to do was commit suicide, which she tried to do by cutting the forearm of her right hand with a razor blade. The girl was lucky, she remained alive and she is now receiving psychiatric help.

Another case. An unidentified man, during a conversation in the "WhatsApp" messenger with a young girl who is a citizen of the Republic of Belarus, prompted the latter to send him her nude photo. Then, under the threat of posting this image on the Internet, he demanded to shoot a video with her participation, in which she had to perform various sexual acts in relation to herself. Frightened by threats, the child obeyed the requirements of the criminal.

Not only children, but also adults fall into this trap when the interlocutor, who initiated intimate communication on a romantic dating site, begins to extort money from the victim under the threat of distributing photos and videos that became accessible to him or her during the communication, which the victims want to keep secret or when, after viewing pornographic sites, their users receive on the phone or computer notifications on the need to pay a fine for viewing the specified content, allegedly from the police.

3 CONCLUSION

Summing up the above, it should be said that, like any phenomenon in life, the development of the Internet and computer technology has its positive and negative sides. Cybercrimes are, unfortunately, the flip side of the coin of the scientific and technological progress of society. In this regard, successful counteraction to the spread of this category of crimes requires efforts not only from the competent law enforcement authorities, but also from ordinary people who should observe basic precautions while on the World Wide Web.

RESUMO

O artigo apresenta informação acerca da competência e a base legal do Gabinete do Procurador Geral da República da Bielorrússia na esfera da cooperação legal internacional em cibercrimes. Examina os

tipos de crimes em que os cidadãos da República da Bielorrússia costumam ser vítimas cometidos utilizando-se o ambiente de internet.

Palavras-chave: *Convenção de Budapeste. Cibercrime. Internet. Assistência mútua legal. Procurador Geral da República da Bielorrússia.*

REFERENCES

Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. Signed on January 28. Strasbourg: 2003.

Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Signed on January 22. Minsk: 1993.

Convention on Legal **Assistance and Legal Relations in Civil, Family and Criminal Matters**. Signed on October 7. Chisinau: 2002.

Convention on Cybercrime. Signed: on November 23. Budapest: 2001.

Materials of the practice of the International Legal Department of the Prosecutor General's Office of the Republic of Belarus for the provision of mutual legal assistance. *In* **criminal matters**.

https://www.coe.int/en/web/cybercrime/cybereast.

http://www.prokuratura.gov.by/en.