УДК 343.3
DOI: 10.17277/voprosy.2015.03.pp.240-246

FRAUD IN "CYBERSPACE" AS A TENDENCY OF CRIME SOPHISTICATION

O. M. Dementyev, M. M. Dubrovina, M. A. Mentyukova

Tambov State Technical University, Tambov

Reviewed by Doctor of History, Professor V. V. Nikulin

Keywords: Criminal Code; criminal liability; "cyber fraud"; fraud; identity theft; Internet crime; Internet; media.

Abstract: The authors analyzed the main causes of fraud in cyberspace. The concept of fraud was examined from various perspectives, including the practices of foreign countries and Russia. The various schemes of fraud using the Internet were explored.

The changes in the legislation related to this kind of crime were studied. The ways of solving the problems were proposed.

All spheres of society are undergoing constant changes in the twenty first century. In the light of the alterations of international information relations, relations in the economic sphere, the political sphere and the cultural sphere will active develop too. The global and domestic information networks, such as the Internet, are developing. With their improvement the popularity of electronic commercial activity increases. Against this background different kinds of e-crime arises. Particularly fraud is thriving, namely, its special kind – "cyber-fraud". Following factors can be reasons for this:

1. Economic reasons include unemployment at the enterprises, crises and growth of taxes. In connection with this, "easy money" obtained through the Internet is becoming popular.
2. Political reasons include changes of the political programs in different spheres, changes of authorities, which entails social instability and lawful nihilism.
3. Social-psychological reasons include the excessive trustfulness of people. They can be defined as derivatives from the economic reasons.

Дементьев Олег Михайлович – старший преподаватель кафедры «Уголовное право и прикладная информатика в юриспруденции», e-mail: lexdom@mail.ru; Дубровина Мария Михайловна – студентка; Ментюкова Мария Алексеевна – кандидат юридических наук, старший преподаватель кафедры «Уголовное право и прикладная информатика в юриспруденции», ТамбГТУ, г. Тамбов.

Many works of different authors are devoted to this problem: V. Sabadash, A. Kazimirko-Kirillova, E. Kasperskiy, and also an enormous quantity of the websites in the Internet [1]. This question received wide acceptance not only in the domestic legal and the informational practices, but also in the foreign ones. The leading countries of the world, such as the USA, Great Britain, France, Italy, etc are engaged in the fight against the new phenomenon. In view of the varying interpretations it is required to identify the most common definition of "fraud", and then to give a logical definition to the concept "cyber-fraud".

Therefore, based on the above, the goal of this article can be defined into following problem aspects:

1. Identification of the concept "fraud" as the legal institute in criminal law.
2. Revelation of adaptation of this concept to the "cyber-space".
3. Development of proposals for updating the legislation, including international, related to the regulation of this type of encroachment on property relations.

The concept of fraud (swindling) in national legal systems

According to Art. 159 of the Criminal Code, fraud (swindling), that is, stealing of other people's property or the acquisition of the right to other people's property by deception or breach of trust; the deception is understood as a deliberate distortion of the truth (active deception) and omission of the truth (passive deception). In both cases, the victim deceived transfers his property to a fraudster (swindler) [2].

In national legal systems the definition of fraud, as a rule, is connected with the fraud or breach of trust.

In particular, the Criminal Code of Canada assumes responsibility for fraud in different spheres: Articles 340, 342, 342.1 governs liability for fraud with various kinds of documents, credit cards and computer information. Articles 380-382 regulate liability for fraud in the property sector [3].

In Europe, a fairly broad definition of fraud is given in the German legislation. Paragraph 263 of the Criminal Code provides punishment for the one who "with intent to deliver himself or a third party illegal property benefits will cause damage to the property of another by introducing them to error, to maintain it in error, giving false facts as true, or distorting or hiding the true facts" (i.e., cause an ax to grind through deception property damage) [4].

Considering these definitions, we can say that they are all associated with the concepts of swindling "fraud", "misleading", "encroachment on the property". This is the basic definition of fraud (swindling). It is well known that most of the concepts appear from the practical actions or events. These basic features can be transferred to the plane of informational networks and define the concept of "cyber-fraud".

Thus, the "cyber-fraud" is the theft of another's property or buying another's property by fraud or breach of trust, while under the deception is understood as a deliberate distortion of the truth (active deception) and omission of the truth (passive deception) committed in the information field (space).

International practice knows a huge number of examples of "fraud", including "cyber-fraud". There are various schemes of it, namely, auction fraud, fake cashier's check, credit card fraud, debt elimination debt on bank cards, the

circuit Parcel Courier Email, fraud in providing services to the depositary identity theft, online extortion, investment fraud, lottery, Nigerian letter or "419", phishing, Reshipping, spam [5].

The most common types of this fraud through online auctions are more common in Romania. Persons of the Internet auctions offer the demanded product. They allow victims to send half of the funds as prepayment, and the other half when the goods will be delivered [5].

Sellers from the United States who advise the victim to send money to a business partner, lawyer, sick relatives, family members, etc., usually located in one of the European countries are often involved in online auctions. Money is usually transferred via Money Gram or Western Union wire transfer. Funds can be picked up anywhere in the world, using personal information about its owner. There's no need to provide money transfer control number (PNC) or the answer to any security question, as many actors have personal information of victims. Money sent via wire transfer, which leaves little room for victims to protect themselves. There is an increasing trend towards using online transaction system of cash payments. Most importantly, these wire transfers go through major banks in the United States and then are sent to Bucharest, Romania or Riga, Latvia [5].

Another best known method of fraud is "debt elimination". Debt elimination schemes are usually associated with advertising websites in the United States, directed to the "legal" way to get rid of mortgage loans and credit card debt. Most often, all that is required from the participant is to transfer $ 1,500 to $ 2,000, as well as all the information about the participant credit and a special power of attorney to transactions concerning the real estate of the participant on his behalf. Then the person issues bonds and notes to the lenders who claim to legal satisfaction repayment of debts of the participant. In exchange, the participant is obliged to pay a certain percentage of the value of the debt satisfied. The potential risk of identity theft from crimes related to the scheme of debt elimination is extremely high because the participants provide all your personal information to the executor [5].

The first and most famous type was the scheme called "Nigerian letter or 419", named for breach 419 of the Nigerian Criminal Code, "419 scam" is fraud related to the receipt of payment for winning the lottery, inheritance, etc. By mail, email or fax the potential victim receives a message. This communications from individuals representing themselves as Nigerian or foreign governmental officials and offering the recipient the "opportunity" to share in a percentage of millions of dollars for their help in placing large sums of money in overseas bank accounts. Payment of taxes, bribes to public officials, and attorneys' fees are often described in great detail with the promise that all expenses will be reimbursed as soon as funds will be transferred out of the country. The scheme is based on credible willingness of the victim to send money to the author of the letter in several stages with an increase in the cost of the next phase for several reasons [5].

"Investment fraud" is used by a great number of fraudsters. In 1997 the case was brought by the Federal Trade Commission (FTC). FTC against Audiotex Connection, Inc, CV-970726 (EDNY), specifically engaged in a scam in which Internet users were invited to view or get free access to images of

models of computers. February 10, 1998, FTC issued a statement before the Senate Subcommittee on Investigations of the Government, that when the audience tried to gain access to these images, modems of their computers were secretly cut off from their local Internet service providers (ISP) and were connected to the Internet via expensive international modem connection. About 38 000 consumers fall for this scam, losing $ 2.74 million [5].

The "IFCC 2001 Internet Report" revealed that 81 % of those committing acts of fraud were believed to be male, and nearly 76 percent of those allegedly involved in acts of fraud were individuals. According to the report, California, Texas, Florida, New York, and Illinois were the states in which half of the perpetrators resided. The report also provided a shocking example of just how difficult a task tracking down those involved in Internet fraud can be. According to the report, out of the more than 1.800 investigations initiated from complaints during 2001, only three arrests were made [5].

Based on the very disappointing statistics a question arises: what to do with such a growing number of "cyber-fraud" crimes and how to resolve it? Improve the states' legal framework or to make technical changes and improvements of the World Wide Web?

In most of the countries there are general rules of law regulating fraud.

Above reference to the provisions of the Criminal Code of Canada were cited.

French Penal Code assumes responsibility for fraudulent activities as well in the field of entrepreneurship.

The overall rate of fraud in the Criminal Code of Germany (§ 263 of the Criminal Code of Germany), supplemented by special rules (§ 264 – a grant by deception; § 265 – insurance fraud), and specialized rules which extend the criminal law prohibition of actions which are not covered by the concept of fraud (§ 263a – computer fraud; § 264a – stock fraud; § 265a – abuse with guns; § 265 – credit fraud) [4].

Having considered all these rules of law, we can conclude that they are regulating the material (real) crimes of pecuniary nature, but not in the Internet. Legal norms sanctioning for "cyber-fraud" are finalizing and developing in the United States, Romania, Germany. This is due to the difficulties in determining the composition of the crime and in 75 cases out of 100 are anonymous (perpetrator is unknown).

In the international IT sphere the organization that are directly involved in struggle with "cyber-fraud" are founded." There are specialized organizations to combat fraud. The EU has engaged in this European Anti-fraud Office, EBBM (OLAF, Eng. European Anti-Fraud Office), but the competence and regulations of any one of these organizations are not included tasks to monitor and curb "cyber-fraud".

The concept of "cyber-fraud" in Russia

The concept of "cyber-fraud" is not directly enshrined in Russian legislation, but Art.159.6 "Fraud in the field of computer information is a theft of another's property or acquisition of another's property by entering, deleting, blocking, modification of computer information or otherwise interfere with the

operation of means of storage, processing or transmission of computer data or information and telecommunications networks" [2].

In Russia, there are also precedent cases of "cyber-fraud." So, 24-year-old resident of Tver programmer Alexander Panin, who was temporarily in the Dominican Republic, was extradited to the United States and now forcibly held in this country. Young Russians suspected of large-scale "cyber-fraud," according to an e-edition of "Russian planet." Panin's relatives noted that he had been already held in prison for a month, without providing any formal charges. US authorities have refused to comment on the situation, and the Russian Foreign Ministry is silent. All documents in the case of a programmer are in the courts under the "top secret." They presented to the arrested a warrant of December 20, 2011, signed by a judge of the State of Georgia, which states that he is suspected of major financial fraud. Ostensibly Panin via the Internet could break passwords of several American banks and stolen from their accounts about 5 millions of dollars. However, all data on the Tver hacker given by "Russian planet" in no way confirmed. Name of the arrested Russian is not mentioned on the website of Interpol in Georgia judicial district where the case is heard, explain that all materials are "sealed at the request of both parties" [6].

ITAR-TASS reports that the court in New York January 4, 2012 Russia's Vladimir Zdorovenin sentenced to three years' imprisonment for "cyber-fraud" and identity theft. The period of Zdorovenin in the US custody is counted in January 2012, so he would have to spend in custody for another two years. After that, he will be deported to Russia. Zdorovenin was arrested in Switzerland in March 2011 and then extradited to the United States. According to US authorities, he and his son Kiril in 2004 organized a criminal group which was engaged in the theft of personal information of cardholders. As a result, the victim suffered damage amounting to several hundred thousand of dollars. In addition, according to the prosecution, Zdorovenin and his son engaged in fraud in the banking sector by buying and selling shares on behalf of others in order to have an impact on their value. During the trial in February 2012 Zdorovenin pleaded guilty to two of the nine counts. Protection requested to appoint him as a punishment, not more than two years in prison, taking into account his remorse and lack of previous convictions [7].

In Russia the combat of fraud is mainly conducted by staff of the units to combat economic crime.

Due to the increase of crimes in the IT sphere Department "K" with the territorial divisions was established by the Ministry of Internal Affairs. These units are entrusted to struggle with the "cyber-fraud".

One of the main reasons forcriminal torts as a result of fraudulent activities using the Internet is anonymity (or the opportunity to participate under a nickname), of the contracting parties in transactions on the Internet.

In this regard, we do not support the point of view according to which transactions carried out anonymously or under a nickname shall be recognized as lawful in cases when they are executed at the time of their commission, if it does not require notarization, or their state registration, or registration of purchased goods. The necessity of legalization of such transactions exists in connection with a wide spread of them, including contractual relations, complicated with the electronic components and the regulatory consolidation of

proposed rule would remove uncertainty in this area and fill gaps in the legal regulation.

From the above it can be concluded that the legal framework in Russia, the EU and the US is underdeveloped in sphere of the Internet – crime, namely in the area of "cyber-fraud". In connection with this most of the countries in the world tend to create a relatively independent branch of law that can regulate all kinds of crimes on the Internet [1].

For creation of this branch it is necessary:

– to develop under the auspices of the United Nations legal framework in the form of an international Convention on cyber-fraud, as nowadays such crimes across international borders and for successful combating them, they could be attributed to International Convention offenses. This Convention would be the basis for the introduction into national law similar standards.

– to create certain international bodies to monitor crime on the Internet, with increased enforcement activities, or the creation of departments on the basis of European Anti-fraud Office, EBBM (OLAF, Eng. European Anti-Fraud Office);

– to continue the development and strengthening of specialized units combating certain types of crime on the Internet on the basis of the Interior and the Federal Security Service in Russia.

With the introduction and development of public services the issue of protecting the rights of citizens and legal entities from cyber-crooks is especially acute.

References

1. Ashchin E.N. Zakon i Pravo (Law and legislation), 2002, no. 10, pp. 8-54.
2. Sobranie zakonodatel'stva RF (Corpus of Legislative Acts of the Russian Federation), 1996, no. 25, art. 2954.
3. http://laws-lois.justice.gc.ca/eng/acts/C-46 (accessed 26 December 2014).
4. Sunchaleva L.E., available at: http://aldebaran.com.ru/publications/7318 (accessed 26 December 2014).
5. http://www.ic3.gov/crimeschemes.aspx (accessed 26 December 2014).
6. http://newsland.com/news/detail/id/1221816/ (accessed 26 December 2014).
7. http://mywebs.su/blog/safety/12056.html (accessed 26 December 2014).

References

1. Ащин, Е. Н. Правовое регулирование электронного бизнеса / Е. Н. Ащин // Закон и Право. – 2002. – № 10. – С. 8 – 54.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства РФ. – 1996. – № 25. – Ст. 2954.
3. Criminal Code (R.S.C., 1985, c. C-46) [Электронный ресурс]. – Режим доступа : http://laws-lois.justice.gc.ca/eng/acts/C-46 (дата обращения: 26.12.2014).
4. Сунчалева, Л. Э. Мошенничество в современном законодательстве некоторых зарубежных стран [Электронный ресурс] / Л. Э. Сунчалова // Aldebaran.com.ru : сайт. – Режим доступа : http://aldebaran.com.ru/publications/7318 (дата обращения: 26.12.2014).
5. Internet Crime Schemes [Электронный ресурс]. – Режим доступа : http://www.ic3.gov/crimeschemes.aspx (дата обращения: 26.12.2014).

6. Обвиненный в кибермошенничестве россиянин «засекречен» [Электронный ресурс] // Newsland : информ.-дискус. портал. – 31 июля 2013. – Режим доступа : http://newsland.com/news/detail/id/1221816/ (дата обращения: 26.12.2014).

7. Суд Нью-Йорка приговорил россиянина к трем годам лишения свободы за кибер-мошенничество [Электронный ресурс] // MyWebS : новостная сеть блогов. – Режим доступа : http://mywebs.su/blog/safety/12056.html (дата обращения: 26.12.2014).

Развитие мошенничества в киберпространстве как тенденция совершенствования преступности

О. М. Дементьев, М. М. Дубровина, М. А. Ментюкова

ФГБОУ ВПО «Тамбовский государственный технический университет», г. Тамбов

Ключевые слова: Интернет; интернет-преступность; мошенничество; кибермошенничество; средства массовой информации; Уголовный кодекс РФ; уголовная ответственность; хищение персональных данных.

Аннотация: Проведен анализ основных причин мошенничества, и в частности кибермошенничества. Рассмотрено понятие мошенничества в различных зарубежных странах и России. Проанализированы различные схемы мошенничества с использованием сети Интернет. Рассмотрены тенденции трансформации законодательства, регулирующего привлечение к ответственности за указанные преступления. Предложены пути решения вопросов по данной проблеме.
