Advances in Social Science, Education and Humanities Research, volume 447
Proceedings of the International Scientific Conference on Philosophy of Education, Law and Science in the Era of Globalization (PELSEG 2020)

Judicial Support of High-Tech Crime Research

Vladimir Yuryevich Golubovsky
Faculty of Law
Russian State Social University
Moscow, Russia

Igor Yurievich Nikodimov
Faculty of Law
Russian State Social University
Moscow, Russia
inikodimov@rambler.ru

Elena Anatolyevna Mironova
Faculty of Law
Russian State Social University
Moscow, Russia

***Abstract* — The future is developing at a continuous pace. The main areas of modern technological advances cover space, genetics, food production and telecommunications. While mankind sees the first two trends evolving in the positive direction, there is a growing public concern over food production as experts appear to be increasingly alarmed over food quality. This is due to the fact that in increasing the productivity of food production, modern corporations downgrade the quality of food products in order to boost their profits. However, experts expect most abuses to occur in such an industry as telecommunications in the very near future.**

Keywords — jurisprudence in the field of high technologies, telecommunications industry, high tech fraud, personal data protection.

I. INTRODUCTION

The scientific and technological revolution kicked off in the 1960s. First of all, this had to do with the introduction of cybernetics into scientific, technical and technological processes. The mid 1980s introduction of personal computers into science and industry only served to accelerate the process of the scientific and technological revolution. In their turn, wireless telecommunications boosted this process even further in the 1990s. The technical breakthrough in broadband speed access in the zero years led to the present day situation [1].

This situation is determined by the presence of high-speed data transmission capabilities and digital data processing, as well as remote data processing and transmission.

What awaits us in the near future?

Today, scientists have invented supercomputers, whose data processing speed is computationally sufficient not just to calculate everyday or social processes, but also cosmic processes in time periods estimated in millions and billions of years.

On the other hand, the process of transhumanism has begun to be developed. Human organ transplantation that took off in this decade is booming. The next few years will see a major breakthrough in this area.

CCTV cameras have begun to be introduced in the cities on a massive scale, with the data being processed by both centralized digital clusters and local information processing centers to address specific local issues. Micro digital cameras are expected to be introduced into the human body in the very near future with ensuing unexpected legal results and consequences.

The introduction of bank cards in the 1980s as an alternative to the paper money circulation ushered in an era of personal data digitization and concerns major features of human social life. More personal data including people's health information is expected to be digitized in every country in the very near future.

Telecommunication companies also use their SIM cards as bank cards and consider developing them as personal data storage.

At the same time, the current state of scientific and technological progress leads to changes in production relations, which entail changes in social relations and legal relations.

In addition, the functional remoteness of all scientific and technological developments enables various types of data, cash and other financial transactions to be transmitted across sovereign states' borders without any impediment, which violates the law of each of these independent countries.

First of all, it is necessary to consider the current state of legal relations involving the use of computer information. This has to do with the fact that among all the above elements of scientific and technological progress, computers were the first to be introduced and have the longest recorded history of interaction with humans, this is the reason why the legal relations involving the use of computer data have been well studied and developed.

II. METHODOLOGY

This research in the methodical plan is the analysis of judicial and investigative methods, practice of application of the Russian legislation in economic sphere of action. The

following methods are used: statistical, comparative and lawful, sociological. On the basis of the results, key results were formulated which allowed one to define reasonably signs of the crime connected with corruption in the considered sphere, criminalistic considerable information which, first of all, contains documents of the organizational and financial nature.

III. Results and Discussion

The first positive impressions about computer use were overshadowed by the ease with which it was possible to steal information stored in them. Basically, this type of offense involved white-collar crimes and personal data theft. According to E.G. Kuznetsova [2], computer fraud should be attributed to a special type of swindling because it does not involve deception as a major component of conventional fraudulence. Theft is committed by using various organizational and technical instruments.

The current Criminal Code of the Russian Federation contains a number of interrelated fraud rules [3]. In the first place they include the general fraud rule (Article 159 of the Criminal Code of the Russian Federation), as well as special rules on fraud in various fields (Article 159.1-159.6 of the Criminal Code of the Russian Federation).

Also worth noting is that special fraud norms originated from relatively recent legislative changes [4]. This innovation was caused, first, by the criminogenic patterns of the market including a variety of fraudulent tricks, emergence of endless new types of sharp practices and constant adaptation to the changing economic organization of production and exchange. This pattern has greatly impacted the complication of the immediate objects of fraud.

Second, as noted in the literature, the general provision of Article 159 of the Criminal Code of the Russian Federation did not fully take into account the specifics of certain economic relations, and therefore did not provide proper protection of the interests of citizens affected by fraudulent actions [5]. On the one hand, we saw the Russian Federation introduce a legal norm regarding computer data theft which came into effect in 2012 [6].

It is a welcome development, but quite a few lawyers disagree with the qualifications of this article as swindling which means that legal practice has not yet been fully established. On the other hand, the recently introduced article 159.6 has not yet been tested against various kinds of abusive practices in order to confidently state that it provides just regulation of the legal norm in this kind of social relations. For example, according to this article, downloading a file from a computer can be construed as a computer information fraud, committed by a group of people upon a preliminary collusion and lead to five years of forced labor. Data about its side effects is most likely to be obtained and evaluated by experts who will have yet to comprehend and correct the legal norm in the near future.

Article 228.1 “Illegal making, sale or transportation of narcotic drugs....” works in the same way. 2018 saw the number of suppressed illicit drug trafficking cases decrease exponentially. The Federal Service for Drug Control has proved to be less efficient over the past 10 years due to some possible mistakes that were committed during the reorganization of this drug enforcement agency. However, farmers are forbidden to grow the garden variety of poppy in their vegetable gardens for personal use, in other words, they are facing the consequences of the agency’s failure to professionally limit illicit drug trafficking.

Humanized in a similar way was Article 282 "Incitement of Hatred or Enmity, as Well as Abasement of Human Dignity». It transpired that many PC users had been put in prison for merely reposting a message in social media. However, quite a few politicians appear on TV with openly racist appeals and none of them is charged with the violation of this article.

The next large-scale high-tech crime is related to unauthorized use of bank cards. Long gone is the time of bank card thefts and unauthorized charges on card owners’ accounts. This is because previously all it took a card owner to make a transaction using bank cards was put his John Hancock. However, the amounts of money fraudsters had appropriated by using stolen bank cards were so enormous that banks had to introduce mandatory PIN and CVV codes. It should be recalled that Russia was one of the first countries to tighten the payment procedure by making cardholders enter a PIN code when using their bank cards.

Today, however, we are seeing a new spike in bank card frauds as new swindling technologies appear.

For example, in Ukraine, bank card thefts using new fraudulent schemes have become much more frequent lately. The fraudsters do not ask for a PIN code or a CVV code. After visiting the Pension Fund to file their documents for a pension plan, some Ukrainians begin to receive suspicious phone calls. In one case, a fraudster introduced himself as an employee of the National Bank and suggested to the pensioner that he verify his position on the bank website. “You need to give your full card number to check the information, as well as the two phone numbers you call most often. You do not need to submit your PIN code or your CVV code or your code word. Take the card into your hand and give its full number” - the callers would say. This is how scammers steal your phone number. “The card number and two phone numbers are all they need in order to have a SIM card reissued and the victim's SIM card blocked”, a security expert says.

Having obtained the bank card number and the phone number from the duplicate SIM card, the scammers gain full access to the money on the account. It goes without saying that neither the PIN code nor the CVV code protect your savings any longer. All one has to do is to have your bank card information and personal data in order to have the bank reissue your bank card and provide access to people’s savings [7].

Similarly, Russian hackers send SMS messages to potential victims containing reference to the federal law on blocking a bank card due to the fact that the recent operation seems somewhat suspicious to the bank. The bank card holder is then asked to call back to confirm his transaction and give

his personal data. After sending his personal information, this person may consider his money as good as lost.

According to the estimates of Attack Killer, a Russian cybersecurity company, about one hundred people have already suffered from the new fraud scheme with a total damage worth about 2 million rubles.

Experts explain the success of the swindling scheme by the fact that fraudsters track and masterfully copy the real changes in the way banks work.

Another way scammers use to get money from people's bank cards is setting a skimming device on a cash machine. This skimmer reads the magnetic tape of a payment card. If the card is not protected with a chip, the scammers create a duplicate and withdraw cash from ATMs that do not require additional identification.

How not to be trapped. You should set a maximum limit on your cash withdrawal. Once skimmers start to cash smaller amounts, you will have enough time to contact the bank and block your account.

Another trick is called Cash Trapping – sticking the ATM cash dispenser with a Scotch tape. Therefore, when a customer keys in the amount he wants to withdraw, the money remains inside the ATM. If the victim writes off this failure as a technical problem and leaves, the scammer quickly walks up to the machine and takes it all.

How to avoid the trap? If you have any technical problems, contact the bank.

Fraudsters also use a method called "A Telephone Call from a Bank Specialist". First, he presents himself as a bank employee and tells you that a large amount of money has been transferred to your account. However, the operation cannot be completed because of the limit the customer has set.

Then the scammer asks you to go to a nearby ATM with his mobile still in his hand and to follow the instructions that will cheat the potential victim of all his money. If this trick does not work, "an investigator" calls the potential victim a week or two later and explains the situation: we are after a gang of scammers who have stolen money from many people. Will you please help the investigation and dictate your card number, its expiration date and CVV code.

Typically, con men come up with convincing legends that people buy quite easily without suspecting any fraud. However, the purpose of such maneuvers is to obtain personal data from your card in order to withdraw your money later.

How to avoid the trap? Bank employees never ask their customers to give them customers' personal data. In this situation, it pays to keep your personal information to yourself.

There are quite a few ways of withdrawing money from people's bank cards illegally. When bank cards first began to be introduced in the 1980s- the 2000s, the talk was about how poorly protected these cards were and when a card was compromised it was, as a rule, the bank that suffered most. Today banks have created a serious transaction protection system making it almost impossible to steal money from one's account unless fraudsters have access to a bank client's personal data. Therefore, the main danger lies in the loss of personal data and its acquisition by swindlers. Both a bank and a client may be responsible for personal data loss; however, it is only a client that had access to some of his personal data such as the PIN code, etc.

Therefore, the main short-term challenge is to protect one's personal data. In 2006, the Russian Federation adopted a law on personal data protection which began to have a good effect at the beginning. Soon it transpired that too many interested parties had developed an overwhelming desire to possess Russian citizens' personal data. The result is that it is impossible to get a job in any organization or to formally enter into any serious labor relations unless a client gives his "voluntary" consent for the transfer of his personal data to the legal entity under a non-divulgation clause. However, this clause offers no guarantees and the latest crime stats show an upward trend in the fraudulent use of personal data.

The next most important fraud in the field of telecommunications involves SIM card use. For example, the following type of fraud has become widespread in Ukraine [8]:

A victim's telephone number alone does not open bank accounts, but after learning his card number, scammers gain access to the victim's finances. The fraudster calls his mobile operator claiming he has lost his SIM card and gives his telephone number.

To have his phone number restored, the scammer must provide the operator with the information about his most recent phone calls and the date of the recent top-up. That is why the evil doer himself calls the victim from different phone numbers before the scam and puts a small amount of money on the account.

How not to be trapped. If you received some money on your account, and then received three phone calls by mistake, be sure to inform the mobile operator about your suspicion of having been duped.

Smishing SMS messages. A swindler pretending to be a prospective buyer finds a product he is interested in, contacts its seller and agrees to purchase it without any further questions. After receiving the victim's bank account details the fraudster sends him a smishing message of the transaction instead of the money.

How not to be trapped. Keep on checking up your account and do not trust SMS messages.

In addition, telcos themselves often use such a gimmick as unsolicited services. An SMS message is sent about a free additional service. But in its large text body there is a bottom line saying that the service is free for the first week, and after the first week the company will start charging you for the service on a daily basis. It is until at best one or, as a rule, two or three months later that the client finds it out. Meanwhile, his money is as good as lost – and there is no one to answer for it. This is the so-called gray high-tech scam. However, this "gray fraud" is termed as established business practice.

Another type of fraud is e-wallet fraud. On classified advertisements websites fraudsters cheat people out of their expensive items instead of money. A fraudster finds an attractive product he wants to get, then he copies the ad and sends it on his own behalf after marking down the price considerably.

There is bound to be someone who would gladly catch the bite and decide to buy the item cheaply without knowing it is merely a scam copy. He transfers the money to the first seller's bank account, but the item goes straight to the scammer instead.

How not to be trapped. Always use P.O.D. In this case, the seller will receive his money once you have inspected the item and remained satisfied with the purchase.

The most popular fraud scheme is required prepayment. For example, you are looking for a rare car part. A go-between contacts you and offers his help in return for a small advance payment – a mere10-15 %, in order to be convinced of the customer's serious intentions.

An endless line of lame excuses follows this: holidays, lack of time and will-give-it-back-tomorrow promises.

How not to be trapped. Do not send prepayment to unverified individuals and companies, such as those you have found on notice boards.

Another way of using high technologies for criminal purposes is Dark Net, a hidden part of the Internet. Quite recently, on October 10, 2018, a major case detective, Lieutenant Colonel of the Ministry of the Interior, who investigated high-profile white-collar crimes, was murdered.

When the criminals were apprehended it transpired that the murder had been ordered through Dark Net, which means that the hidden part of the Internet is made a good use of to do all kind of criminal transactions.

To pay for these hidden contracts, they use e-wallet technologies, which transfer money for a committed crime. Payment is made with the help of bitcoins using blockchain technology. These technologies are in great demand in the criminal world as they allow making payments without disclosing its beneficiaries. The creators of Dark Net alone can reveal these data - the very reason why they have devised the system in order to keep payments and money transfers hidden from disclosure.

In order to study the legal problems created by modern technologies that have changed social relations, but for which no new legal rules have been made or fully completed, relevant studies have been conducted including statistical research and public opinion polls [9]. With the aim in mind, an opinion poll was conducted among 150 students at the Russian State Social University. Questions were asked about what side effects will soon be relevant in the legal field following the introduction of high technologies.

The student survey showed the following negative consequences of high-tech implementation:

1. Increased dissemination of false information - 19%.
2. Growing crime, hacking and theft result in a new type of crime - computer fraud - 19%.
3. Decline in culture and social intercourse - 16%.
4. Poorer medical health and aggravated environmental problems -16%.
5. Computer crimes foster corruption - 7%.
6. Computer crimes promote instability - 9%.
7. Data leaks - 7%.
8. Violation of people's rights when filming on the streets - 3%.

IV. CONCLUSION

The future is developing at a continuous pace. The main areas of modern technological development include space, genetics, food production, and telecommunications. While humankind sees the first two trends evolving in the positive direction, there is a growing public concern over food production, as experts appear to be increasingly alarmed over food quality. This is because by increasing the productivity of their food production modern corporations downgrade the quality of food products in order to boost their profits. However, most crimes occur in such an industry as telecommunications.

References

[1] I.Yu. Nikodimov, "Information Law and Information Society: a General Description of its Formation and Foundation Stages, Regulated Social Relations," Legal Science: History and Modernity, vol 2, pp. 88-95, 2016.

[2] E.G. Kuznetsova, "Computer Fraud: Qualification Issues," Criminal Law, vol. 4(15), pp. 87-90, 2017.

[3] A.V. Maiorov, "Criminal and Legal Characteristics of Fraud: Qualification Issues," Proceedings of the 68th SUSU Scientific Conference, 2016.

[4] A.G. Bezverkhov, "Fraud and its Types: Issues of Legislative Regulation and Qualification," Criminal Law, vol. 5, 2015.

[5] M.F. Musaelyan, "On Some Problems Associated with Introduction of Special Fraud Elements to the Criminal Code of the Russian Federation," Russian Investigator, vol. 10, 2016.

[6] On Amendments to the Criminal Code of the Russian Federation and Some Legislative Acts of the Russian Federation: Federal Law of November 29, 2012 N207-FZ. The Official Gazette, vol. 49, art. 6752, 2012.

[7] Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ

[8] Retrieved from: www.google.com.ua.meduza.io 2019

[9] I.Yu. Nikodimov, "Topical Issues of Information Law," Bulletin of the Moscow State Linguistic University. Series: Education and Pedagogical Sciences, vol. 763, pp. 147-160, 2016.