УДК 343

А.М. Соловйова
кандидат юридичних наук, доцент,
докторант Класичного приватного університету

ДЕЯКІ АСПЕКТИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ЗЛОЧИНИ ПРОТИ ВЛАСНОСТІ, ВЧИНЕНІ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ, ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА ДЕЯКИХ ЗАРУБІЖНИХ КРАЇН

A. Soloviova
Candidate of Juridical Sciences, Associate Professor,
Doctoral student of Classical Private University

SOME ASPECTS OF THE CRIMINAL RESPONSIBILITY FOR CRIMES AGAINST PROPERTY COMMITTED WITH THE USE OF COMPUTER TECHNOLOGY BY THE LEGISLATION OF UKRAINE AND SOME FOREIGN COUNTRIES

Formulation of the problem. Globalization of law is defined as "the worldwide progression of transnational legal structures and discourses along the dimensions of extensity, intensity, velocity and impact". On the same context, the term of global law means "the setting up of the Institute acknowledges the impact of law across national boundaries and the need to deepen inquiry into comparative approaches to law and legal study."

Global law means also that ""the law and its practice in a global environment", or "a multicultural, multinational, and multidisciplinary legal phenomenon finding its roots in international and comparative law and emerging through the international legal practice that was prompted by the globalization of the world economy" [1].

Steven Shavell, scientist from Harvard uses the term "property rights" to refer broadly to two subsidiary types of rights, possessory rights and rights of transfer. What are often called possessory rights allow individuals to use things and to prevent others from using them. A particular possessory right is a right to commit a particular act or a right to prevent others from committing a particular act. The other type of right associated with the notion of property rights is a right to transfer a possessory right, that is, the option of a person who holds a possessory right to give it to another person (usually, in exchange for something) [2].

The aim of the article is investigate of the criminal responsibility for crimes against property committed with the use of computer technology by the legislation of Ukraine and some foreign countries.

The main results of the study. Revolutionary development of information technologies became a part of our life and simplified it so much that we already cannot do without mobile phones, computers, the Internet etc. At the same time, one should remember that the novelty creates a new field for criminal identify elements instead of defining information.

Crimes committed with the help of information technologies have larger dimensions and complicate investigation in comparison with classical criminal methods [3].

What is "property?" The term is extraordinarily difficult to define. One of America's foremost property law scholars even asserts that "[t]he question is unanswerable." The problem arises because the legal meaning of "property" is quite different from the common meaning of the term. The ordinary person defines property as things, while the attorney views property as rights. Most people share an understanding that property means: "things that are owned by persons." For example, consider the book you are now reading. The book is a "thing." And if you acquired the book by purchase or gift, you presumably consider it to be "owned" by you. If not, it is probably "owned" by someone else. Under this common usage, the book is "property." In general, the law defines property as rights among people that concern things. In other words, property consists of a package of legally recognized rights held by one person in relationship to others with respect to something or other object [4].

The processes of informatization of society generate a number of issues related to the qualifications of fraud. Article 17 of the Constitution of Ukraine provides that one of the most important of functions of state include ensuring information security. Therefore the problem of the criminal-legal qualification of fraud committed with the use of computer technology is of particular relevance. In legal literature, there is no single point of view on the question of criminal and legal assessment of criminal acts committed with the use of computer technology.

For years, criminals have been using discarded credit card receipts, bank statements, tax notices, and other bills (often found in the trash) to gain the personal information necessary to assume another person's identity. However, on today's electronic playing field, these criminals have used technology to devise cunning new methods of theft in the form of cyber crimes. Now, computer hacking and email scams known as phishing are included among the risks of sharing information online. Computer hackers are able to enter areas of the Internet where they are prohibited and hack in to another computer network. Once they are inside a computer's network, they are able to view documents, files, and confidential data and use it for their own personal gain. Phishing, on the other hand, is a method in which people are duped into providing their own personal data to a thief who is posing as a legitimate business or agency. Both of these cyber crimes have been steadily on the rise in recent years. In fact, according to the Wall Street Journal, there were more than 9.9 million cases of identity theft last year in the United States [5].

In foreign science criminal law, computer fraud is one of the most rapidly increasing forms of computer crime. Computer fraud is also commonly referred to as Internet fraud. Essentially, computer/ Internet fraud is "any type of fraud scheme that uses one or more components of the Internet-such as chat rooms, e-mail, message boards, or Web sites to present fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme" [6].

According to part 3 of article 190 of the Criminal Code (hereinafter - CC) of Ukraine fraud committed in respect of a gross amount or by unlawful operations involving computerized equipment shall be punishable by imprisonment for a term of three to eight years [7].

The difficulty of linking the relatively well understood legal definition of 'theft' to a information-centric concept of 'identity' is because the informational characteristics of identity (non-exclusivity) renders the assignment of the status of property (and hence theft) complex; because one person is falsely using the identity of the other does not necessarily mean that the victim is deprived of his or her identity. Legal definitions of the constructs of theft and fraud may thus have an impact when considering the use and definition of 'identity theft' and 'identity fraud'. As pointed out in the FIDIS report on the Dutch Penal Code (and this applies to many other criminal codes in the world) theft requires the loss of possession of tangible goods; consequently the applicability of the concept of theft with respect to identity might be limited. Usage of the notion of 'theft' may also undermine the reality that there is not only a criminal but also a civil aspect to identity theft/fraud that may bring with it a tort liability for damages [8].

In the Ukrainian science of criminal law, there is a view that the use of counterfeit means of payment, resulting in a de facto transfer of funds or obtain cash, has qualified on set of crimes stipulated in Articles 200 and 190 of the Criminal Code.

The opposite position is that the term "fraud" is inappropriate for uses in the legal definition of socially dangerous acts, the essence of which boils down to the introduction of changes, damage of computer information in computers, automated systems, computer networks or telecommunications networks with the purpose of taking possession of another's property. The term "deception", especially trafficking "abuse of trust" cannot be used to refer to acts in the form of the introduction of false information into a computer system. Categories such as truth, lies, trust, confidence, etc. characterize the relationship and communication between people. You can not fool the computer or abuse his trust [9, p. 54–55].

We agree with those scientists who believe that at the time the fraud using electronic computer is deceived person who uses the computer to improve their activities. In addition, a convenient point of view of the severity of sanctions on p.3 article 190 of the Criminal Code of Ukraine, this does not always correspond to the social danger of encroachment that contain signs of a crime under this norm.

There are three basic elements of identity: • biometric identity: attributes that are unique to an individual, i.e. fingerprints, voice, retina, facial structure, DNA profile, hand geometry, heat radiation, etc; • attributed identity: the components of a person's identity that are given at birth, including their full name, date and place

of birth, parents' names and addresses; • biographical identity, which builds up over time. This covers life events and how a person interacts with structured society, including: – registration of birth; – details of education/qualifications; – electoral register entries; – details of benefits claimed/taxes paid; – employment history; – registration of marriage; – mortgage account information/property ownership; – insurance policies; – history of interaction with organizations such as banks, creditors, utilities, public authorities[10].

The definition of identity theft was first codified in 1998 as part of the Identity Theft and Assumption Deterrence Act of 1998 (ID Theft Act). The ID Theft Act made identity theft a stand-alone crime. More specifically, it amended the federal criminal code to make it a crime for anyone to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law[11].

The process of identity theft is recognized when:"criminals acquire key pieces of personal identifying information- such as name, address, date of birth, mother's maiden name, employment information, credit information, and other vital facts in order to impersonate and defraud the victim, this stolen information enables the thief to commit numerous forms of fraud, including taking over the victim's financial accounts: applying for loans, credit cards, and Social Security benefits, purchasing homes and cars and establishing services with utility and phone companies for instance."

Other resources repeatedly indicate almost the same situation: "Identity theft occurs when a criminal steals key pieces of personal identifying information to gain access to a person's financial accounts." In comparison to this, the United States Secret Service defines identity crimes as "the misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity [12].

Identity theft and identity fraud are terms that are often used interchangeably. Identity fraud is the umbrella term that refers to a number of crimes involving the use of false identification— though not necessarily a means of identification belonging to another person. Identity theft is the specific form of identity fraud that involves using the personally identifiable information of someone else. Both identity fraud and identity theft are crimes often committed in connection with other violations, as mentioned above. Identity theft, however, may involve an added element of victimization, as this form of fraud may directly affect the life of the victim whose identity was stolen in addition to defrauding third parties (such as the government, employers, consumers, financial institutions, and health care and insurance providers, just to name a few). This report, however, maintains a focus on identity theft rather than the broader term of identity fraud [13].

Identity theft is not just a problem in its own right. It also has ramifications for other types of crime. United States and Canadian law enforcement agencies report a growing trend in both countries toward greater use of identity theft as a means of furthering or facilitating other forms of fraud, organized crime (the bulk

of identity crime is committed by organized crime) and terrorism. Especially troubling is the now established link between identity theft and national security [14].

In Europe, Mitchison describe it rather narrowly: 'Identity theft, in what in this paper is called its "paradigm" form, occurs when one person – in this study a „rogue" – obtains data or documents belonging to another – the victim – and then passes himself off as the victim.' This description, like the former, covers only the unlawful use of identifying data from another person. This is a rather narrow view, since credit-card fraud, for example, can also be committed by generating a nonexisting credit-card number. In other words, one can equally – or perhaps not quite equally – well commit identity fraud without 'stealing' someone else's identity. Therefore, 'identity fraud' can be conceived of as a broader term than 'identity theft'. In a study by the UK Cabinet Office, this is described functionally: ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent [15].

Identity fraud can roughly be described as the unlawful changing of someone's identity. Rost, Meints, and Hansen distinguish four closely related subcategories of identity change: identity takeover, when someone takes over the identity of another person without that person's consent; identity delegation, when someone uses someone else's identity with that person's consent; identity exchange, when two or more people, with mutual consent, use each other's identity; identity creation, when someone creates the identity of a non-existing person [15].

The French Criminal Code contains a specific provision for identity theft (Article 434–23). However, conducts which do not constitute by themselves a crime remain unpunished. This is for instance the case of fraudulent use of emails by third parties for, for example, affiliating the victim to a political party or other associations. Similarly, phishing cannot be currently punished under Criminal Law if not followed by potential initiation of criminal prosecution against the victim. In order to solve this legal loophole, the creation of a new crime that would punish identity theft in electronic communications is currently being discussed by the French Parliament. If approved, the act (known as LOPPSI 2) would introduce a new article into the Criminal Law Code [8].

Conclusions. Thus, the study showed that the norm of p. 3 art. 190 of the Criminal Code "fraud committed by illegal transactions using computerized equipment" do not correspond to the actual level of development of information and public relations and needs to be improved. It is necessary to study and borrow positive experience of foreign countries. It is expedient to study criminal law of Estonia which establishes responsibility for computer criminal acts (Articles 206–208), such as computer sabotage, damaging of connection to computer network, spreading of computer viruses.

REFERENCES

1. Deab Morad Yasin. From Legal Translation to Legal Globalization: Globalization of Criminal Laws to Counter Global Crimes / Morad Yasin Deab Al-Refo, Raed S.A. Faqir // Electronic resource: http://www.ijssh.org/vol6/657-B00010.pdf

2. *Shavell Steven*. Economic analysis of property law / Steven Shavell // Electronic resource: http://www.law.harvard.edu/programs/olin_center/papers/pdf/399.pdf

3. *Shukan Alya*. Criminal Law Problems of IT-Crimes in Kazakhstan and Turkey/ Alya Shukan, Yavuz Erdogan // Electronic resource: http://www.idosi.org/mejsr/mejsr17(12)13/21.pdf

4. *Sprankling John*. Understanding property law / John G. Sprankling // Electronic resource: https://urbanforensics.files.wordpress.com/2012/09/sprankling_understandingpropertylaw.pdf

5. Identity Theft: Evolving with Technology // Electronic resource: https://www.sjpd.org/BFO/Community/Crimeprev/crimeprevention%20forms/Identitytheft.pdf

6. *Kunz Michael*. Computer Crime and Computer Fraud / Michael Kunz, Patrick Wilson // Electronic resource: http://www.montgomerycountymd.gov/cjcc/resources/files/computer_crime_study.pdf

7. The Criminal code of Ukraine // Electronic resource: http://zakon3.rada.gov.ua/laws/show/2341-14

8. *Robinson Neil*. Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report / Neil Robinson, Hans Graux, Davide Maria Parrilli, Lisa Klautzer, Lorenzo Valeri // Electronic resource: http://ec.europa.eu/dgs/home-affairs/e-library/documents /policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

9. *Muzyka A.A., Azarov D.S*. Zakonodavstvo Ukrayiny pro kryminalnu vidpovidalnist za «kompyuterni» zlochyny: naukovo-praktychnyy komentar i shlyakhy vdoskonalennya. – K.: Vyd. PALYVODA A.V., 2005. – 120 s.

10. Identity fraud: a study // Electronic resource: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf

11. Putting an End to Account-Hijacking Identity Theft // Electronic resource: https://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

12. Identity Theft in Electronic Environment: Does the current approach to the penal legislation of European Union and Lithuania adequate for combating cybercrime? // Electronic resource: https://www.duo.uio.no/bitstream/handle/10852/34432/174180.pdf?sequence=1

13. *Finklea Kristin*. Identity theft: trends and issues / Kristin Finklea // Electronic resource: https://www.fas.org/sgp/crs/misc/R40599.pdf

14. Identity theft: introduction and background // Electronic resource: https://cippic.ca/sites/default/files/bulletins/Introduction.pdf

15. *Koops Bert-Jaap*. Identity Theft, Identity Fraud and/or Identity-related Crime / Bert-Jaap Koops, Ronald Leenes // Electronic resource: http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf

Соловйова А.М. Деякі аспекти кримінальної відповідальності за злочини проти власності, вчинені з використанням комп'ютерних технологій, за законодавством України та деяких зарубіжних країн

У статті досліджено деякі аспекти кримінальної відповідальності за злочини проти власності, вчинені з використанням комп'ютерних технологій, за законодавством України та деяких зарубіжних країн. Автором проаналізовано основні точки зору вітчизняних і зарубіжних вчених на проблему кримінальної відповідальності за вчинення таких видів злочинів.

Ключові слова: *кримінальне право, комп'ютер, злочини проти власності, крадіжка, шахрайство.*

Соловьева А.Н. Некоторые аспекты уголовной ответственности за преступления против собственности, совершенные с использованием компьютерных технологий, по законодательству Украины и некоторых зарубежных стран

В статье исследованы некоторые аспекты уголовной ответственности за преступления против собственности, совершенные с использованием компьютерных технологий, по законодательству Украины и некоторых зарубежных стран. Автором проанализированы основные точки зрения отечественных и зарубежных ученых на проблему уголовной ответственности за совершение таких видов преступлений.

Ключевые слова: *уголовное право, компьютер, преступления против собственности, кража, мошенничество.*

Soloviova A. Some aspects of the criminal responsibility for crimes against property committed with the use of computer technology by the legislation of Ukraine and some foreign countries

The article examined some aspects of the criminal responsibility for crimes against property committed with the use of computer technology by the legislation of Ukraine and some foreign countries. The author analyzed the main points of view of domestic and foreign scholars on the issue of criminal responsibility for the commission of such crimes.

Keywords: *Criminal law; Computer; Crimes against property; Theft; Fraud.*

Стаття надійшла до редакції 20.07. 2016.