PRACTICAL ASPECTS OF CRIMINAL AND LAW CHARACTERISTICS OF CYBER CRIMES IN UKRAINE

Natalya Ustrytska, Lviv State University of Internal Affairs
Lesya Skreklia, Lviv University of Trade and Economics
Oleksandra Kochyna, Chernihiv National University of Technology
Igor Kopotun, Academician Stepan Demyanchuk International Economic and Humanitarian University
Olena Honcharenko, Research Institute for private law and entrepreneurship named after Academician F. G. Burchak NPR of Ukraine

ABSTRACT

The article summarizes the theoretical generalization and solves the scientific problem, which consists in identifying the peculiarities of the criminal law qualification of crimes in the sphere of use of electronic computers (computers), systems and computer networks and telecommunication networks, and development based on it proposals for improvement of the current legislation. The general theoretical aspects of criminal legal qualification of crimes in the sphere of use of electronic computers (computers), systems and computer networks and telecommunication networks have been established. It is established that the criminal legal qualification of these crimes acts as an instrument of realization of lawfulness in criminal proceedings. The view was maintained that such a qualification is a qualitative reflection of the study of the circumstances in which a socially dangerous, unlawful, guilty, criminal act was committed.

Keywords: Cyberspace, Cybercrime, Information Space, Organized Computer Crime, Virtual Gangs.

INTRODUCTION

Ensuring information security in Ukraine is one of the most important functions of the state, because the well-being of the nation depends on the information component. Today, the state of criminogenic situation requires the development and implementation of measures to prevent criminal encroachment on objects in the use of electronic computers, systems, computer networks and telecommunication networks.

Because of socio-economic problems, Ukraine is far behind in developing countries of the Convention on Cybercrime. Cyberwarfare, cyber terrorism, cyber espionage have become commonplace, so crime in the information field is a significant threat to national security in the economy.

Information spaces touch virtually every sphere of human life, and therefore, crime takes on new, more sophisticated forms. Crimes in the use of electronic computers (computers), systems and computer networks and telecommunication networks are a serious threat to existing

public relations, because rapid informatization of society is, as an activator of new forms of criminal behavior.

Crime is a human act, so it is inherent in all those objective and subjective features that characterize human behavior (physical properties-one or another movement or its absence, the use of physical, chemical, biological and other laws of the surrounding world; psychological properties-a manifestation of consciousness and will, a certain motivation of behavior, its purposefulness).

The crime can be called an encroachment on relationships that reflect the overriding interests and are therefore protected by criminal law. Objective patterns of development of society, its needs and interests are a measure of the value of human behavior, its conformity or inconsistency with these needs and interests, so crime is always antisocial behavior.

REVIEW OF PREVIOUS STUDIES

Pursuing the criminal law qualification of the crimes, on the basis of the circumstances under which they were committed, the norms for which the liability for the crime is assumed are selected (Drobyazko et al., 2019a, 2019b, 2019c). The preliminary conclusion is that there was a criminal act, not an administrative misconduct, a civil offense, a disciplinary misconduct or any other offense.

Assumptions are made about the application of certain criminal rules and state that what is done does not fall under the signs of other criminal rules (Sunde, 2017). This is the initial stage of criminal qualification.

Thereafter, a correlation is established between the actual features of the offense and the crime composition provided for in the criminal law (Lusthaus & Varese, 2017). It is important that the evidence base is lawfully collected, because only then will it have the status of lawfully obtained evidence.

Thereafter, from the criminal law chosen for the legal assessment of the offense, the characteristics characterizing the committed assault are distinguished, and in the presence of several alternative features, the features characteristic of the assault to be qualified are selected (Miquelon-Weismann, 2017). In this process, use the structure of the crime, which is devoted to the next chapter of scientific work.

The next step is to consolidate the results of the qualification, it occurs in the procedural documents and involves at least three actions (Hilorme et al., 2019a, 2019b): a statement of the facts of the case; drawing up of the qualification formula; statement of the charges.

A statement of the facts of the case is to formulate the actual composition of the act (Hui et al., 2017). For this purpose, the most important facts are selected from the facts established in the case;

At the same time, despite the importance of these and other scientific developments, today there are many problems in the criminal law qualification of crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks. In particular, there is no comprehensive criminal-law analysis of the qualifications of crimes in this area. The above testifies to the relevance and timeliness of the chosen topic of scientific research, the need to study the criminal qualification of criminal offenses and to build a model of crime prevention in this area.

METHODOLOGY

In the course of the research, general scientific and special methods, methodological principles and approaches of legal science were used, which were used to ensure the reliability of the obtained results, conclusions and recommendations of scientific knowledge. The basis of the study is dialectical method, as a general scientific method of knowledge of social and legal phenomena in their contradictions, development and changes, which made it possible to determine the peculiarities of criminal-law qualification of crimes in the field of use of electronic computers (computers), systems and computers and telecommunication networks. The logical-semantic method is used to improve the conceptual understanding of criminal qualification of crimes and to study the main features of criminal law qualification of cybercrime.

RESULTS AND DISCUSSIONS

The high degree of public danger of crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks is caused by the following factors:

1. Intensive introduction of information technologies and processes based on the use of electronic computers in many fields of human activity;
2. High scale of the efforts of criminals in this area;
3. Relative accessibility for a wide range of persons with specialist knowledge and techniques required to commit a crime.

Consequences of actions such as damage (damage) caused (or can be caused) to social relations can be material (damage having personal (physical) or property) or intangible (damage in political, organizational and social spheres).

Public danger, as a material sign of a crime, consists in the fact that the act either causes harm to the relations protected by the criminal law or contains a real possibility of causing such harm. This is an objective property of crime, a real violation of the relations existing in society. The emergence, change, loss of social danger of action are caused by objective patterns of social development, an inseparable connection with those socio-economic processes that take place in society. In Part 1 of Art. 11 of the Criminal Code of Ukraine (Criminal Code of Ukraine, 2001) public danger as a mandatory sign of a crime is only called, its meaning is not disclosed by law. Public danger as a sign of crime is assessed at two levels:

1. Legislative when the legislator criminalizes a certain socially dangerous act;
2. When the investigating body, the investigator, the prosecutor, the judge assess the public danger of the crime.

Therefore, social dangers belong to valuation concepts. The criterion for the assessment of public danger, its degree are the objective and subjective signs of crime: the object to which the crime is committed, the consequences, the mode of committing the crime, the form of guilt, motive, purpose and more. Only an assessment of their totality can reveal the objective, real danger of the crime.

In our opinion, the measure of public danger of crimes in the use of electronic computers, systems and computer networks, telecommunication networks is determined by the value of the information on which the criminal act is committed (by the act or by inaction), and the mental attitude of the subject to the consequences of his act, the motive and purpose pursued by the offender.

The unlawful feature of a crime is its unlawfulness. As a formal sign of a crime, unlawfulness means its presence in criminal law. Criminal unlawfulness is closely linked to social danger: it is a subjective expression of objective, real danger of action for public relations, its legislative evaluation. Therefore, criminal law-a legal, legal assessment of public danger - is enshrined in law. It is the social danger, its degree, which determines the objective limits of unlawfulness, beyond which the question of criminalization cannot arise. Allocation of criminal wrongdoing by law as a mandatory feature of a crime is a specific expression of the principle of legality in criminal law: Only a person who has committed a socially dangerous act, which is prescribed by law as a crime, is liable to criminal responsibility and punishment. Criminal law provides a comprehensive list of crimes. Therefore, if the act is even a danger to society but is not provided for by the law on criminal liability, it cannot be considered a crime.

It turns out that the most important provision about the impossibility of applying the criminal law by analogy to such action, which is not explicitly provided in it, because in accordance with Part 4 of Art. 3 of the Criminal Code of Ukraine the application of the law on criminal liability by analogy is prohibited (Criminal Code of Ukraine, 2001).

RECOMMENDATIONS

Due to the absence of legal acts that would directly determine the rules of operation of computers, systems and networks. we propose to make a judicial or enforceable interpretation in the form of explanations, for example at the level of the Resolutions of the Plenum of the Supreme Court of Ukraine.

We offer a contingent of computer technology users, offering free results on the latest criminal performance from 16 years to 14 years.

We propose to supplement the existing forms of guilt - criminal negligence, which would include signs of indirect intent and criminal overconfidence (frivolity), this is exactly the form of guilt inherent in Art. 361-1 of the Criminal Code of Ukraine. It makes sense to supplement section XVI of the Criminal Code of Ukraine with qualifying warehouses for committing computer crimes by organized groups and criminal organizations, enhancing criminal liability for the use of official position, not only to Article 362 of the Criminal Code, but also to other rules of the section. It is advisable to carry out qualification on a set of norms of the Criminal Code under Article XVI of the Criminal Code and Article 255 of the Criminal Code of Ukraine and against the background of increased social danger.

CONCLUSIONS

On the basis of the conducted researches an attempt was made to improve the criminal-legal qualification of crimes in the sphere of the use of electronic computers (computers), systems and computer networks and telecommunication networks. The most problematic issues in conducting the criminal legal qualification of cybercrime were identified and the following measures aimed at solving them were developed:

the use of personal data with criminal intent, such as hacking databases, which results in the copying of personal information of bank customers, which can lead to more serious consequences. It is proposed to introduce Article 361-3 of the Criminal Code of Ukraine *"Illegal copying of restricted information stored on electronic computers (computers), automated systems, computer networks or on such media".* The development of information technology has led to the emergence of new criminal acts, which are currently absent in the Criminal Code of Ukraine. However, given the absence of unlawful acts in the law, it is impossible to prosecute a person. It is proposed to supplement the norms of Title XVI of the Criminal Code of Ukraine with the most common types of international crimes. Cybercrime through a computer on the Internet. The problem is the ambiguity of the application of legislative regulation, where different countries are the place of crime and the place of occurrence of socially dangerous consequences. The status of the legal regime of the Internet is discussed, similar to the status of public areas. In the exercise of criminal legal qualifications, it is necessary to overcome the competition of legal norms of crimes provided for by Title XVI and other sections of the Criminal Code of Ukraine. In cases where the composition of a particular crime covers the act contemporaneous with this crime, provided for in Article XVI of the Criminal Code of Ukraine, and the sanction of the Article of the Special Part of the Criminal Code, a more severe capital punishment is established for this crime than for the act provided for in Article XVI of the Special Criminal Code of Ukraine, such action does not constitute a set of crimes and does not require separate qualification. There will be no set of crimes in cases where the acts committed are envisaged by different clauses of one article, unless those clauses have their own sanctions. If the social dangers of the relationships protected by the additional object are greater than the main object, then the action will form the perfect totality. If the act is an assault on various direct objects of criminal defence, then the act must be qualified according to the rules of the set of crimes. The fate of cybercrime victims remains unresolved. The use of punishment is aimed at preventing the commission of crimes, with the introduction of the Institute of Criminal Offenses, corrections were made to Section XVI of the Criminal Code of Ukraine-increased amounts of financial penalties. However, in most cases the penalty is not applied, or is applied, the funds from which come to the state budget. Compensation to the victim is possible provided that she is sued, but these are rare cases. For the most part, the victim at best receives only moral gain. That is why it is proposed to introduce an indemnity institution for cybercrime in order to compensate materially for the violated rights of victims. In the absence of the required amount, it is proposed to use public works, the funds from which will be transferred to the victims' account.

REFERENCES

Criminal Code of Ukraine. (2001). *Vidomosti of the Verkhovna Rada of Ukraine (VRU), No 25-26.*

Drobyazko, S., Alieksieienko, I., Kobets, M., Kiselyova, E., & Lohvynenko, M. (2019a). Transnationalisation and segment security of the international labor market. *Journal of Security and Sustainability Issues 9*(2), 1-20.

Drobyazko, S., Bondarevska, O., Klymenko, D., Pletenetska, S., & Pylypenko, O. (2019b). Model for forming of optimal credit portfolio of commercial bank. *Journal of Management Information and Decision Sciences, 22*(4), 501-506.

Drobyazko, S., Makedon, V., Zhuravlov, D., Buglak, Y., & Stetsenko V. (2019c). Ethical, technological and patent aspects of technology blockchain distribution. *Journal of Legal, Ethical and Regulatory Issues*, *22*(2S), 1-11.

Hilorme, T., Perevozova, I., Shpak, L., Mokhnenko, A., & Korovchuk, Y. (2019a). Human capital cost accounting in the company management system. *Academy of Accounting and Financial Studies Journal, 23*(SI2), 1-11.

Hilorme, T., Sokolova, L., Portna, O., Lysiak, L., & Boretskaya, N. (2019b). Smart grid concept as a perspective for the development of Ukrainian energy platform. *IBIMA Business Review, 19*(1), 1-11.

Hui, K.L., Kim, S.H., & Wang, Q.H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly, 41*(2), 497-516.

Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice, 23*(1), 1-11.

Miquelon-Weismann, M.F. (2017). The convention on cybercrime: A harmonized implementation of international penal law: What prospects for procedural due process? In *Computer Crime* (pp. 171-204). Routledge.

Sunde, I.M. (2017). *Cybercrime law.* Digital forensics.