RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
MARCH 2021

DOI: 10.5281/zenodo.4639702

The Making of Fraudulent Economic Operations and Identity Theft as Cybercrimes in Romania

Dan Cristian

"Dimitrie Cantemir" Christian University of Bucharest, Faculty of Juridical and Administrative Sciences – Law, Bucharest, Romania, danrcristian@gmail.com

ABSTRACT: In the 21st century, information has gained a huge value, mainly because the human activities have transitioned from the physical world to the digital one. Among these activities, we can find the innovated economic one, represented by the accumulation of capital in virtual accounts handled and insured by the banks. Another transitioned element consists of the social processes, this being done nowadays on different networks and mobile applications. Due to the fact that humans have created the systems by which our personal data is protected and which assure ones right of property over a digital monetary transaction alongside the right to a private life when it comes to a conversation on platforms with one or more people, these programs are susceptible to fraudulent activities done by individuals with high informatics skills. The current paperwork will analyze from a legal approach the crimes which can be committed in regards to the above-mentioned aspects. The branch of criminal law will serve as the main building block for reaching valid conclusions.

KEYWORDS: cybercrimes, criminal law, psychology, identity theft, victims, social networks, criminal resolution, data protection systems, the subjective criminal side

Cybercrimes: notion and elements

The concept of cybercrime can be defined as that criminal act done in an informatics environment, by which all the necessary resources are consumed in order to achieve the illegal objective that it is brought into reality by the will of the author or the desire of some else, serving as means of completion for the main criminal. For both situations (author and accomplice) the individual fully knows the damage that he/she is about to inflict on the victim. In the end, he/she will be held responsible, thanks to the judicial process (Mitrache C. and Mitrache Cr. 2019, 248).

From the perspective of the Criminal Law, the cybercrimes can be committed only with direct intention, due to the fact that for the completion of such an act a well-prepared way of operation is necessary, this including the most favorable moment and the complexity of constructing the means of execution. In this manner, the illegal act has a well-drawn reason and a final objective, a clear vision (Ristea 2020, 116).

When it comes to the cause which can remove ones criminal liability, on a general level, they cannot be raised in this case, because there is no real justification in completing this action: no immediate danger which needs to be stopped, cannot be removed by any other method and with the manifestation in the virtual space. In other words, the psychical presence of the danger and the temporal extent of the executed act makes the justification of being a legal behavior almost impossible (Coman 2020, 87).

The guilty cannot state that he was in a state of complete intoxication (drunk or drugged) when doing the criminal act, due to the fact that these types of crimes require the author to be conscious about the final result and to possess high intellectual resources in order to complete the resolution, attributes which are shut down by the usage of such substances (Acsinte 2012, 131).

On the other hand, there are scenarios where the responsible person needed to act this way as a result of a moral of physical constraint, him being the only one capable at that time to commit the cybercrime. The constraint can be done by creating a threat towards the family members or towards the friend circle of the hacker. Also, the imminent danger can be imposed on the cybercriminal himself. In this case, the author can raise the fact that he had to

complete the criminal action due to the danger posed by the threat, and thus we are in the presence of a cause that can remove the possible punishment (Udroiu M. and Trancă A. and Trancă C. 2014, 217).

There are times when, even if an individual commits a cybercrime with a clear intention an a well desired goal, the person doing it can suffer from a factual error towards the correct reality, especially in regards of his target and if the error has an essential role, this can lead to the removal of the criminal liability (Boroi 2019, 253).

Completing fraudulent economic operations as cybercrimes

By completing fraudulent economic operations in the virtual world we can understand the stealing, falsification or misrepresentation of any data with a fiscal attribute, in an online environment, the information being connected with any financial element belonging to a person or any legal entity, with the purpose of the criminal to take this capital into his own possession (Ioniță 2018, 126).

These cybercrimes are recognized in the specialized doctrine as qualified versions of theft and embezzlement, thanks to the common elements present in the criminal resolution and the methods used for the achievement of the goal, the main distinction being that certain skills, experience and instruments are necessary for the completion (Pașca, Ciopec and Roibu 2013, 203).

By referring to the subjective part of the financial cybercrimes, the motive shows the psychical state of the author that lead to the desire to accumulate capital, the end scope being the criminal resolution of completing the operation (Butoi 2019, 425).

When it comes to the unity of the crime, the fraudulent bank operations done in an informatics sphere can be separated by the number of execution acts into simple crimes and continuity crimes. A special case is represented by the crimes done in a continued form (Stănilă 2020, 355).

In normal cases, the person which commits to cybercrimes chooses to transfer the bank data in stages, usually more subjects of the law suffering from a loss of small amounts in their accounts. The victims generally do not realize that they have become a target or simply choose not to inform the proper authorities, based on the consideration that the damage dealt is too insignificant to worry about. Since the response of the injured party is usually absent, the criminal continues his/her behavior, thus we can see a cybercrime done in a continuous form (Duțu 2013, 312).

There are scenarios in which the active subject of the crime commits the act in a simple form by extracting a large amount of money from the victims account. This is done either due to the lack of experience of the author, either because of an unrealistic sense of safety generated by the false confidence in his/her abilities or even because that individual has a general lack of attention and manifests negligence when planning (Butoi T., Butoi I., Butoi A. and Put 2019, 217).

In order for someone to successfully complete a cybercrime, he/she needs to have proper knowledge in the domain of Information Technology, and modern equipment which can repel the devices used for prevention and protection. Devices used to counteract the defense mechanisms are instruments that hide the informatics protocol and programs which permit the hiding and relocation of the signal. Using such elements qualifies the crime to its aggravated form (Udroiu M., Trancă A. and Trancă C. 2014, 318).

Due to the complexity of the operation, the methods used, the necessary intellectual capacity and the required equipment, cybercrimes done for economic reason can only be completed with a direct intention (Sergiu and Șerban 2020, 178).

Generally, this type of criminal behavior does not have any cause for justification so that one should be released from the criminal liability, the exception being an external

constraint towards the hacker or his/her kin or friends. This constraint can be in the form of a threat or a direct physical action (Hotca 2020, 318).

Identity theft as a cybercrime

The identity theft in the context of cybercrimes represents the taking without consent of the personal data belonging to another subject of the law with the intention to complete actions or activities in their name, the end goal being the obtaining of material benefits and/or the defame of the victim (Acsinte 2012, 149).

The criminal resolution, in this case, is completed with intention and it is specifically destined to a certain person or a group of people, based on economic, political or social reasons and consists in assuming the identity of the respective individual or legal entity (Udroiu M., Trancă A. and Trancă C. 2014, 277).

In the last period, identity theft as a cybercrime has become a common practice in the virtual world, especially on social platforms, where, even if no harm is intended, some users pretend to be someone else, creating fake accounts known as "avatars", or they choose to pose as their friends based on a personal reason, not necessary a criminal one.

Also, from the sphere of identity theft we can observe the completion of economic illegal operations. In order to steal the financial data from the users' bank account the first element to be gathered is their personal data, these can be extracted from the device which the victim uses to store their information (Gheorghe and Ivan 2019, 395).

A special case and of high importance for the current analysis is represented by the stealing of personal data from a person in order to force the victim into providing the criminal with sexual favors. Generally, this type of activity targets women, which think that on the other side of the computer, is a different individual. Due to this false impression, they are convinced to complete several improper acts in front of their webcams. After the display has been recorded, the information will be used by the real hacker in order to make the victim perform sexual activities or to give them other kinds of benefits (material or monetary) (Leș 2018, 342).

The motive for this type of crime can consist in the creation on a social platform of a fake account which poses as a political party with the purpose to distort the public image of that entity. A false identity can also be created for the spreading of anti-Semite, extremist or violent ideas.

Identity theft can be utilized for monetary reasons. Such is the case if an individual chooses to pose as a public figure and then organizes campaigns to grow his own capital (Acsinte 2012, 168).

For these types of cybercrimes, the only way that the criminal liability can be removed is for the victim to agree with the actions taken by the author (Neagu 2020, 297).

Conclusions

In our century the majority of the activities performed by humans has transitioned from a physical environment to the virtual one, especially when it comes to the economic, social, political, religious and educational ones.

For the above mentioned to function properly several protection systems regarding personal data had to be implemented.

These systems, being made by man, are not perfect and can be hacked. The most common targets are the network protecting the economic and political domains.

The action of fraud against the systems which protect the data is present in the category of cybercrimes regulated by the criminal law, and the individuals which perform such an activity are held responsible.

Cybercrimes can be committed only with direct intention, due to the fact that for the completion of such an act a well-prepared way of operation is necessary, this including the most favorable moment and the complexity of constructing the means of execution.

From the sphere of these criminal conducts, the most relevant ones are the completion of economical fraudulent operations and the identity theft.

The action with a purpose represented by the high jacking of an economic operation in the virtual environment is also part of the identity theft cybercrime category.

When it comes to the theft of computer data with an economic nature, there is no cause which can be raised in court in order for the criminal liability to be removed, the only case by which the author can be exempted from the responsibility of his/her action being a scenario in which he was constraint to act this way for the benefit of another.

In the case of an identity theft with the focus on stealing the personal data of a certain subject of the law, a cause for the removal of the criminal liability is the existence of the consent towards these actions, given by the victim.

The illegal activities done in the informatics area are categorized in their aggravated form, due to the fact that a high qualification and intellectual capacity are necessary for completion.

Nowadays, a large concern is placed on data security with the objective of prevention and fight against cybercrimes, on a national and international level. However, there will always be persons able to hack in the protection systems no matter their quality of creation. In this manner, every citizen has to inform himself correctly in regards to the navigation on the internet and to properly follow the instructions provided by the specialists in order to assure a good defense against cybernetic attacks.

References

Acsinte, M. 2012. *The Rights of the Informational Society*. Bucharest: Universul Juridic Publishing House.

Boroi, A. 2019. *Criminal Law. Special Part*. Bucharest: C. H. Beck Publishing House.

Butoi, T. 2019. *University Treatise on Forensic Psychology*. Bucharest: Prouniversitaria Publishning House.

Butoi, T., Butoi I., Butoi A. and Put C. 2019. *Behavioral Analysis from the Perspective of Forensic Psychology, Victimology and Forensic Tactics*. Bucharest: Prouniversitaria Publishing House.

Coman, V. 2020. *Crimes on Cyberspace Place*. Bucharest: Universul Juridic Publishing House.

Duțu, A. 2013. *Forensic Psychology*. Bucharest: Universul Juridic Publishing House.

Gheorghe, I. and Ivan C. 2019. *Criminal Law. Special Part*. Bucharest: C. H. Beck Publishing House.

Hotca, M. 2020. *Handbook of Criminal Law. General Part. 3rd Edition*. Bucharest: Universul Juridic Publishing House.

Ioniță, G. 2018. *Crimes in the Field of Cybercrime*. Bucharest: Universul Juridic Publishing House.

Leș, A. 2018. *Psychopatology of Sexual Fantasies. Methodology of Investigating Criminological Psychology*. Bucharest: Universul Juridic Publishing House.

Mitrache, C. and Mitrache Cr. 2019. *Romanian Criminal Law. General Part*. Bucharest: Universul Juridic Publishing House.

Neagu, N. 2020. *Criminal Law. General Part*. Bucharest: Universul Juridic Publishing House.

Pașca, V., Ciopec F. and Roibu M. 2013. *Economic Crime in the Crisis Context*. Bucharest: Universul Juridic Publishing House.

Ristea, I. 2020. *Criminal Law. Special Part*. Bucharest: Universul Juridic Publishing House.

Sergiu, B. and Șerban A. 2020. *Criminal Law. Special Part*. Bucharest: Universul Juridic Publishing House.

Stănilă, L. 2020. *Criminal Law. General Part II*. Bucharest: Universul Juridic Publishing House.

Udroiu, M., Trancă A. and Trancă C. 2014. *Computer Crimes in the New Criminal Code*. Bucharest: Universul Juridic Publishing House.