The Requirement to Deceive – a Serious Shortcoming of the Bulgarian Computer Fraud Regulation

Die Täuschungsanforderung - ein ernster Mangel der bulgarischen Computer-Betrugsverordnung

Ralitza Dimitrova

Faculty of Management, Technical University of Sofia
Sofia, Bulgaria, rvd@tu-sofia.bg

***Abstract* —** Digital transformation is impossible without effective protection against cyber crime. Different forms of unlawful conduct committed through new technologies pose a serious threat against information society. The present article deals with computer-related fraud – one of the most widely spread cyber crime offences which causes significant losses to individuals, businesses and whole countries. The computer fraud provisions in the Bulgarian Criminal Code are analyzed in relation to a brief comparative analysis of the computer fraud regulation in another six Member States of the European Union. Some serious shortcomings in the Bulgarian criminal law regulation of computer fraud are pointed out and proposals for amendments are made.

***Zusammenfassung* —** Digitale Transformation ist ohne wirkungsvollen Schutz gegen Cyberkriminalität unmöglich. Die verschiedenen Formen des rechtswidrigen Verhaltens, die durch neue Technologien begangen werden, stellen eine ernsthafte Bedrohung für die Informationsgesellschaft dar. Der vorliegende Artikel befasst sich mit Computer-Betrug - ein der am weitesten verbreitete Verbrechensverhalten, das erhebliche Verluste für Einzelpersonen, Unternehmen und ganze Länder verursacht. Die Computerbetrugsbestimmungen im bulgarischen Strafgesetzbuch werden in Bezug auf eine kurze Vergleichsanalyse der Computerbetrugsverordnung in weiteren sechs Mitgliedstaaten der Europäischen Union analysiert. Es werden auf einige ernsthafte Mängel in der bulgarischen Strafrechtsregulierung von Computerbetrug hingewiesen und Vorschläge für Änderungen unterbreitet.

I. Introduction

It seems that at every turn, someone is talking about digital transformation [1]. But digital transformation is not just a modern word. It is a phenomenon intended to benefit our lives in almost every aspect. Even to the casual observer, the existence of technology trends such as hyper connectivity, smart devices, and cloud computing is obvious [1]. Digital transformation changes both the way the public sector operates and the business is exercised. Through e-government people are allowed to communicate with state and local institutions in a fast, easy and convenient way. In the private sector more and more individuals and companies use new technologies to buy and sell goods and services, make electronic payments, check their bank accounts, etc. Digital transformation allows companies to improve how they currently operate, create new business models and sources of value, and maintain a competitive advantage [1] and thus benefits also customers of goods and services.

Unfortunately, it is clear that information technologies are used not only for good purposes – to get the mankind's life better, but also by criminals for the commission of various wrongful acts with adverse consequences. Infringement of the inviolability of correspondence, child pornography, fraud, hacking, cracking – all these, and many other crimes are committed through new technologies. Individuals and companies suffer monetary and moral damages unseen before. Therefore, security in the information society and digital transformation are at great risk. Experts point out that the automation of virtually all business processes and the increasing digital connectedness of the entire value chain create agility, but they also significantly raise cyber security risks and threat levels [2]. Cyber security has become a key strategic priority for digital business and is a topic we need to be open about if we want to succeed in digital transformation [3]. Therefore, the reliable cyber security and the effective fight against cybercrime are major priorities for the information society.

The very nature of cybercrime makes it especially dangerous and difficult to tackle. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat [4,5]. It is very important that the majority of countries worldwide implement the main international instrument in this field – the Council of Europe Convention on Cybercrime, and guarantee an effective criminal law protection against cybercrime. EU Member States should also harmonize their national legislations with legal instruments such as Directive 2013/40/EU on attacks against information systems.

Bulgaria has already made a series of amendments to its Criminal Code (BCC) to meet the requirements of both the international and the EU instruments dedicated to the fight against cybercrime. The different cybercrime offences – against the person, against the inviolability of correspondence, against the property, and those representing a direct attack against computer systems and data, were introduced either by

creation of new provisions or by insertion of amendments to already existing provisions of the BCC.

Because of the limited volume of the present paper, it will focus only to one of the so-called computer-related computer crimes – the computer fraud. Nowadays it is more dangerous than traditional fraud – it causes significant losses to both individuals and businesses, even to whole countries. That's why it is very important that criminal law legislations ensure an effective protection of property against fraud committed through new technologies.

In the first part of the paper a brief analysis of the current criminal law regulation of computer fraud in Bulgaria will be made. In the second part the main features of the relevant criminal law provisions in another six EU Member States will be presented. Some of them are old Member States and the other – new Member States of the EU. Besides, five of the said jurisdictions pertain to the Civil Law system and one to the Common Law system, so that the different approaches influenced by the different legal principles and traditions can be taken into account. The third part of the article is dedicated to a comparative analysis where the positive and negative features of the Bulgarian criminal law regulation of computer fraud are pointed out in relation to what are the main trends in the analyzed foreign jurisdictions. In the end the author draws some conclusions based on the comparative analysis and makes some proposals for amendments in the BCC.

II. Criminal Law Regulation of Computer Fraud in Bulgaria

The cybercrime offences were introduced into the BCC by a series of amendments in 2002, 2007 and 2010. For the offences that represent a direct attack to computer systems and data a new chapter "Cybercrime" was elaborated. The other computer-related offences were placed in different chapters of the Code, close to the respective traditional offences, following the principle to arrange the different types of offences in the code according to the character and the importance of the protected social relations. Computer fraud was introduced as article 212a of the BCC, immediately after the traditional fraud and the document fraud

Article 212a BCC describes the computer fraud offence in two main provisions without any special provisions which provide heavier or lighter sanctions.

Under article 212a, paragraph 1 BCC where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computer data or through the use of an electronic signature of another causes him/her or another damage, shall be punished for computer fraud by deprivation of liberty from one to six years and a fine of up to BGN six thousand.

Under article 212a, paragraph 2 BCC the same sanction shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computer data in order to unduly obtain something, that should not go to him.

The following components of the offence are worth noting.

The object of computer fraud is complex and includes different groups of social relations: (1) the relations that guarantee the normal exercise of the property rights; (2) the relations that ensure that people make transfer of property rights upon free decision and clear mind; and (3) the relations which protect computer data against any unlawful manipulation.

The prohibited conduct under article 212a, paragraph 1 reveals the first form of the computer fraud as just a "computerized" version of the traditional fraud – bringing or maintaining of misleading representations [6]. In other words the perpetrator should influence upon another person's mind and deceive him or her about significant elements of an act of transfer of property.

What differentiates computer fraud is the specific method of committing the crime - through a manipulation of a computer data or through the use of an electronic signature of another. The perpetrator either interferes with computer data or uses an electronic signature, thus creating the false impression that the electronic statement is made by the real holder of the signature.

Another component from the objective aspect of the offence is the conduct of the deceived person – guided by the misleading representations he or she performs an act of disposition of rights over real or personal property.

The crime is naturally a result one – to be completed damage must be caused to another's property. Computer fraud is an offence against property which means that the damage must have monetary nature. On the other hand, the description of the offence does not specify the nature of the damage – therefore, causing a moral harm will meet the requirements [6].

The subject of computer fraud is every physical person who is not authorized to introduce the mentioned modifications to the computer data or a person who is not the real holder of the digital signature.

The second form of computer fraud (article 212a, paragraph 2 BCC) has a very broad formulation and criminalizes all kinds of unlawful modifying of existing computer data [6].

This form of the offence requires a criminal result to be completed too – the fact of introducing of the said modifications. However, damage to another person's property here is not needed – it is not an element of the offence.

The perpetrator commits the prohibited conduct without authorization, which is another element in the objective aspect.

The subject is a physical person which has not the right to influence the computer data.

The subjective aspect of the computer fraud requires a direct intent as well as a special aim under article 212a, paragraph 1 (providing a benefit for oneself or another) and a special intention under article 212a, paragraph 2 (unduly obtain something).

The analysis shows that article 212a of the BCC criminalizes an illegal conduct committed through new technologies with the intent to cause an illegal transfer of property in compliance with the aim of the international and EU instruments. However, some studies state that the Bulgarian criminal law provisions on computer fraud are not in full compliance with the Convention on Cybercrime [5,6]. In fact there are some serious shortcomings which make the computer fraud regulation ineffective. They will be discussed below in the light of the comparative analysis.

III. Criminal Law Regulation of Computer Fraud Abroad

Computer fraud is usually described as one of the computer-related traditional crimes [7] or computer based or aided crimes [8]. Deceiving somebody else in order to get for oneself (or for another person) a material benefit is in fact a traditional offence for the criminal law systems. What distinguishes the computer fraud is the use of new technologies for committing the crime and, of course, as we shall see below, the very different mechanism of the crime.

Most criminal law legislations provide for a specific offence criminalizing unauthorized manipulation committed during data processing with the intent to cause an illegal transfer of property (all analyzed legislations below). Other jurisdictions rely on the provisions on traditional fraud to cover also the computer-related fraud (for example France).

Further, the comparative analysis shows that computer fraud is usually regarded as one of the crimes against property, alongside with its predecessor – the traditional fraud. The computer fraud provisions are intended to protect the property interests and naturally the offence is most commonly placed in those parts of the criminal laws which are dedicated to the crimes against property (Germany, Italy, Poland, Romania, Latvia, etc.).

The computer fraud provisions, like other cybercrime provisions, make reference to specific terms connected to new technologies. The most frequently used terms are "computer data" (Poland, Romania) or just "data" (Latvia, Germany); "computer system" (Romania) or "information system" (Italy). Not so long ago in the Latvian Criminal Law was inserted the concept of an "automated data processing system" [9] and the German Criminal Code uses another term – "data processing operation". The Irish provision refers just to a "computer". Generally these terms have a legal definition in the respective piece of legislation. The terms used and their definitions in the national legislations are important aspect of the effective legal framework of fight against cybercrime.

As far as the prohibited conduct is concerned, usually it takes a variety of forms under the analyzed legislations. For example, under the German Criminal Code the perpetrator damages another person's property by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the course of the processing (Section 263a of the German Criminal Code). Under article 640 ter of the Italian Criminal Code the unlawful conduct can take two alternative forms - altering in any way the operation of a computer system or intervening in any manner without the right on data, information or programs contained in a computer system [10]. The forbidden conduct in Poland is any inputting, altering or deleting of computer data or other unauthorized interference with its processing (article 287 1(55) of the Polish Criminal Code); in Romania – entering, altering or deleting computer data or restricting access to such data or hindering in any way the operation of a computer system (article 249 of the Romanian Criminal Code). In Ireland there is a really broad statement which deserves to be mentioned - the offender "operates or causes to be operated a computer" (section 9 of the Criminal Justice (Theft and Fraud Offences) Act of 2001).

In some of the analyzed jurisdictions computer fraud is formulated as a result crime (Germany, Italy, Romania). The offence is completed only when the victim's property has suffered some monetary damage [10,11, 12]. Under the Italian legislation the criminal result has two cumulative components - obtaining a benefit for the perpetrator (or for another person) and causing loss to the victim's property. In some studies it is pointed out that the damage can have also moral nature [10]. Other jurisdictions do not require any materialized criminal result from the offender's conduct (conduct crime) (Poland, Ireland, Latvia). In the opinion of some authors the formulation of the offence as a conduct crime in Poland hinders its effective implementation [7].

A very interesting aspect of computer fraud is the mental element of the offence. All analyzed computer fraud provisions require such element. A direct intent is needed accompanied by a special purpose – "the purpose of making a profit or causing harm" (Poland); "in order to obtain a benefit" (Romania); "for the acquisition of property … in order to influence the operation of the resources thereof" (Latvia) or a special intention – "intent of obtaining an unlawful material benefit" (Germany); "with the intention of making a gain for himself or herself or another, or of causing loss to another" (Ireland). As it can easily be seen in some cases the additional mental element contains alternatively or cumulatively the aim or intention to cause damage to another person's property (Poland, Ireland).

In the end, the comparative analysis will be incomplete without mentioning the special provisions of computer fraud. For example, in a "case of lesser importance" the Polish Criminal Code provides for a lighter penalty than in the main provision (article 287, paragraph 2). The Italian Criminal Code contains a number of special provisions created with a view to different qualifying features: if the offence is committed to the detriment of the State or to another public body; if the quality of an operator of the system is abused; if the offence is committed by theft or by illicit use of digital identity to the detriment of one or more persons (article 640 ter, paragraph 2 and 3). In Latvia the computer fraud under article 177, paragraph 2 of the Criminal Act brings a heavier penalty if it has been committed by a group of persons pursuant to prior agreement, and under article 177, paragraph 3 - if it has been committed on a large scale or if it has been committed in an organized group.

It is worth mentioning that some studies give the German and the Romanian provisions as an example for a model of full alignment with article 8 of the Convention on Cybercrime [5]. Italian and Polish provisions should be praised for the formulation of special descriptions which make possible the differentiation of the criminal liability. Besides, the broad statement of the Irish computer fraud provision should be noted as a good example for a formulation tailored to cover any future technical developments.

IV. Conclusions

On the basis of the analysis of computer fraud regulation in Bulgaria and abroad, the following conclusions can be drawn.

First, the Bulgarian computer fraud provisions are placed in the chapter "Crimes against Property" in the BCC which adequately corresponds to the object of the offence. The comparative analysis already showed that this is also the preferred approach in other jurisdictions. However, there is no reasonable explanation why the document fraud regulation was torn into two parts by inserting the computer fraud offence between the special provisions of document fraud providing for heavier penalties and the special provisions providing for lighter penalties.

Second, the Bulgarian computer fraud provisions use adequate special terms which are in compliance with the main international and EU legal instruments in this field and have suitable legal definitions in the Code (article 93 BCC). It's worth mentioning that some foreign experts also retain that the definitions in the BCC correspond to those in the Council of Europe Convention on Cybercrime [5].

Third, but most important, the present formulation of computer fraud in paragraph 1 of article 212a BCC requires that a physical person must be deceived (the perpetrator "brings or maintains misleading representations in someone"). This is in fact the traditional construction used for the traditional fraud. The problem is that the lawmaker obviously do not realize that the two offences have a very different mechanism – while in the case of the classic fraud the perpetrator needs to influence the mind of a physical person and deceive him or her about one or more substantial elements of an act of transfer of property, in the case of the computer fraud the perpetrator uses the possibilities of new technologies and needs not influence a human mind, only a computer system and/or data, in order to commit the crime. As it was shown above, the analyzed foreign legislations naturally do not require such element. Although their formulations vary

from one another, they obviously correspond far more adequately to the mechanism of computer fraud and to the model provisions of international and EU instruments. Moreover, the difference between the two offences is explained both in the literature and the case law [6, 10, 11, 13,14]. It is pointed out that the core element of the traditional fraud is the deception of the victim, while the computer fraud is committed through an unauthorized influence on a computer system.

While discussing the objective elements of the offence, it's worth mentioning also that foreign legislations often give more general and clear descriptions of the offence which encompass the broad variety of forms and ways to illegally influence computer systems and/or data and allow further technological development. As it was mentioned above some of the analyzed legislations are given as good examples in international studies on cybercrime.

Therefore, exactly the current description of the actus reus should be highlighted as the most serious problem of the Bulgarian computer fraud regulation. The present formulation of article 212a BCC does not correspond to the mechanism of performing the computer fraud by means of new technologies. On one hand, it renders the provisions inconsistent with the current development of new technologies, and on the other – with the trends in the development of the criminal law in this field. As a result, the scope of application of the current provisions is too limited.

Fourth, rather uncommon for the Bulgarian criminal legislation is the lack of special provisions of computer fraud in the BCC. First of all, offences against property offer broad possibilities for differentiation of the criminal liability through elaboration of special provisions with a view to different qualifying features, or, on the contrary, features that decrease the social danger of the respective criminal conduct and justify a lighter penalty. Second, as it was demonstrated above, foreign legislations provide for such special provisions of computer fraud. Such special provisions should be introduced at least for the cases of organized crime, conspiracy, large amount of the damages caused, etc.

In conclusion, the present provisions of the computer fraud in the BCC should be amended in the light of the analysis results above.

References

[1] M. Haendly, "5 Tangible benefits of digital transformation. How digital technologies can increase insight and innovation in your business", *SAPinsider*, vol. 17, issue 2, April 2016.

[2] M. Golz, J. Somaini, "Cybersecurity in the Age of Digital Transformation", *MIT Technology Review Custom*, January 2017.

[3] "Cybersecurity: security risks and solutions in the digital transformation age". Online. Available at https://www.i-scoop.eu/cyber-security-cyber-risks-dx/, 2017.

[4] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Council and the Committee of the Regions. Cybersecurity strategy of the European Union: an open, safe and secure cyberspace /* JOIN/2013/01 final */, 07.02.2013.

[5] Council of Europe, Project on Cybercrime, National legislation implementing the Convention on cybercrime – comparative analysis and good practices, March 2008.

[6] A. Stoynov, *Criminal law. Crimes against property*, Sofia: Ciela, 2006, p. 169 and the following.

[7] A. Adamski, "Cybercrime legislation in Poland", Nicolaus Copernicus University, Poland, 2010.

[8] P. Ryan and A. Harbison, "The Law on computer fraud in Ireland - development of the law on dishonesty", Society for Computers and Law, Arthur Cox, June 2010.

[9] R. Dimitrova and E. Saulitis, "Criminal law framework for combating computer crime in Latvia and Bulgaria", XV International Scientific Conference "Management and Engineering'17", Sozopol, Bulgaria, 2017.

[10] S. Logroscino, "La frode informatica quale autonoma figura". Online. Available at http://www.altalex.com/documents/news/2012/01/02/la-frode-informatica-quale-autonoma-figura-di-reato-rispetto-al-delitto-di-truffa, 2011.

[11] K.J. Heller and M.D. Dubbler, Eds. *The handbook of comparative criminal law*, Stanford: Stanford University Press, 2011, p. 279.

[12] M. Bohlander, *Principles of German criminal law*, Oxford: Hart Publishing, 2008, p. 30, 223.

[13] M.R. Pensabene, "La frode informatica, una figura autonoma di reato". Online. Available at http://www.masterlex.it/approfondimenti/la-frode-informatica-figura-autonoma-reato/, 2017.

[14] Sentenza 24 febbraio 2017 n.9191, Corte di Cassazione della Repubblica Italiana.