Acta Universitatis Danubius
JURIDICA

The Computer System in the Context of the Application of Artificial Intelligence

Adriana Iuliana Stancu[1]

Abstract: The Council of Europe adopted Recommendation R(89)9 on computer crime and published a report containing a minimum list and an optional list of computer crimes. If the member states will take into account these models in the elaboration of national laws, a European harmonization will be achieved regarding computer crime, with special regard to computer fraud. Artificial intelligence (hereinafter abbreviated AI) is the ability of a machine to imitate human behavior, being programmed to think and act like a human. One of the key features of AI is continuous learning, based on external stimuli and information gathered from the environment. AI observes the surrounding reality and acts accordingly, without the need for human help or assistance. Of essence is the fact that from the sphere of information technology that is of interest through their particularities.

Keywords: computer system; AI; technology; computer crime

1. Introduction

It is important to note that without such a computer program, one cannot talk about automatic processing, because it is built in such a way as to act independently of the

[1] Associate Professor, PhD, Faculty of Law and Administrative Sciences, "Dunărea de Jos" University of Galati, Romania, Address: 111 Domneasca Str., Galati 8000201, Romania, Corresponding author: adriana.tudorache@ugal.ro.

user's action. This is not incompatible with the situation where the system is initially given data or instructions by the user, because the program will subsequently operate without human intervention. For example, a mobile banking application is a computer program, which was created and which processes computer data with the help of a programming language called Swift, from an iPhone that represents a computer system. Article 181 para. (2) C. pen. states that "[by] computer data is understood any representation of facts, information or concepts in a form that can be processed by a computer system". The specialized literature also offers examples of relevant computer data in the field of computer fraud, namely the access data for the internet banking account, electronic coins, databases12, etc. In German criminal law, this data is seen as representations of information by continuous signs or functions, which can be encoded as objects or means of processing by a device or which is the result of a processing operation.

2. Interaction of Computer Systems with AI

Regarding illegal acquisition of data, in the German Criminal Code the requirement is restricted only to data that is stored or transmitted electronically, magnetically or that is not directly perceptible in any other way (Zlati, 2020, p. 333). From the definition of the computer program mentioned above, it follows that it falls into the category of computer data. Moreover, it can be considered that computer programs are the most important computer data. This is due to the fact that the other categories of computer data are automatically processed by means of computer programs. The computer program solves a particular "problem" through the set of instructions that underlies it. According to the goal towards which the solution of this problem tends, computer programs can be classified into legitimate and malicious. The latter are based on an illegal use. Examples given in the literature include computer viruses, computer worms and Trojan horse programs (Bulancea, Zlati, & Slăvoiu, 2017). In reality, most computer systems today work through a sequence of processing between computer programs. For example, in order for a computer to start, its operating system (e.g. Windows) goes through a series of processes, starting from the BIOS (Zlati, 2020, p. 333), so that the operating system in turn processes the computer program consisting of the browser - the internet (for example, Google Chrome), in which the user enters the address of a web page (Zlati, 2020, p. 333) to access, without right, the victim's bank account through the internet banking application, where other computer data consisting of the name and access password of that account, in order to finally be modified through another processing of the

computer data consisting of the account balance, through a fraudulent transfer for the purpose of obtaining a material benefit, thus realizing the constitutive content of the crime of computer fraud. Comparing the method of criminalizing computer fraud to the rest of the crimes existing in the criminal legislation, it can be found that it is at the intersection between crimes against patrimony and computer crimes, in Recommendation no. R (89) 9 of the Council of Europe regarding computer crimes [9] showing that the crime comes to fill the gap previously found with regard to fraud-type crimes, respectively the requirement imposed by law the states' regulations regarding the conduct of misleading a person, and regarding crimes of the type of theft or embezzlement, the requirement of the existence of a tangible material object. Moreover, the distinction between computer fraud and deception has long generated a non-uniform jurisprudence, which was eventually removed, as I will show.

With the emergence of new systems, concepts or solutions in the IT field, the ways of committing the crime of computer fraud have diversified, there are some situations in which the apprehension of this crime can generate problems. Among these examples, it is worth analyzing the field of Artificial Intelligence.

Regarding the field of Artificial Intelligence, it should be mentioned from the beginning that this technology belongs to the software component (Stănescu, 2021, p. 2), although it has a source of material inspiration, namely the way the neural networks of the human brain work. Therefore, the discussion is placed in the sphere of the concept of computer data (Husti, 2021). For example, the specialist literature has analyzed the case where artificial portraits of people who do not exist in reality are created using this technology, ruling that the images consisting of portrait photographs, initially offered to the system for processing, constitute computer data (Zlati, 2020). Undoubtedly, the adversarial neural network algorithm (Matthias, 2018) used in this case is a set of instructions that can be executed by a computer system in order to obtain a determined result, as such we can speak of a genuine computer program. The essence of this technology is found in the way computer programs run: for example, with the help of Artificial Intelligence, a mobile phone can classify the photos taken according to what is captured in them, without receiving any instructions from the user. In the same way, materials or drugs can be created by perfecting the molecular structure, identifying cell structures with carcinogenic potential, defects in the material manufacturing process (Malik, Khaw, Belaton, Wong, & Chew, 2022), etc. In the field of computer fraud, Artificial Intelligence is mainly used for preventive purposes. Until the introduction of these

systems, financial institutions carried out prevention measures using a set of rules defined based on the history of fraudulent transactions, so that the system would later issue a warning in case a transaction complies with these rules and thus appears to be a form of fraud. The disadvantage of this type of mechanism is the lack of flexibility, the chronophage character and the fact that it works reactively. For example, we might find based on past experience that when one type of transaction is made from one bank account to a certain other bank account, this transaction is fraudulent because the second bank account has appeared in several cases of fraud over time. In the same way, we could identify a pattern in the behavior of an author of the fraud crime because every time he transfers a very small amount of money to his own account, with the help of a malicious computer program that "rounds" the transactions made. The difficulty arises when the author escapes from this pattern and changes his mode of operation. We previously showed that a computer program solves a given problem using a set of instructions. When the problem to be solved varies over time or changes its parameters according to given circumstances, the original program proves insufficient. Artificial Intelligence solutions can be used to meet these shortcomings (Alpaydın, 2014, p. 2).

In a very simple definition, in the case of Artificial Intelligence, a learning process takes place, without a computer system being programmed in this sense (OECD Recommendation on Artificial Intelligence; Proposal for a Regulation of the Parliament and the Council on Artificial Intelligence). The need for the learning process also appears in those cases where a computer program cannot be used directly to solve a problem, so a set of exemplary data is used as a starting point. In specialized literature (Alpaydın, 2014, p. 2), the situation in which one person transcribes what another verbally communicates was offered as an example. The recognition of words for their subsequent writing is a mental process that cannot be explained in the form of instructions from a computer program. Moreover, even if we admit the possibility of creating such a mechanism, it would only work for the recognition of a single person's voice, by changing the speaker, his accent, making the system ineffective. This is also not true of a person, who can transcribe the voice of a person they understand regardless of accent or tonality. A similar example can be built in the field of computer fraud crimes. Analysis by a member of a banking institution's audit team might reveal a potential fraud, but the process of thought, comparison and perhaps even intuition based on previous experience could never be translated into a computer program, because it involves too many variable parameters. Likewise, manual human analysis also requires a substantial amount of time, with associated high costs. These shortcomings can be combated by training or

learning an Artificial Intelligence program to recognize the relevant data for the action it was programmed to take based on a large amount of data represented by the voices of many people, i.e. transactions performed. However, the computer programs operating on the basis of Artificial Intelligence present shortcomings in the fraud prevention activity, shortcomings that can facilitate the commission of the crime of computer fraud. A first disadvantage is the data imbalance. We have seen that AI programs learn from a given set of data. What is essential in this learning process is their ability to generalize, i.e. to recognize data that, although not similar to that initially provided, has similar general characteristics. It has been shown in the specialized literature (Matthias, 2018; Pozzolo, Boracchi, Caelen, Alippi, & Bontempi, 2017) that if the data offered to learn are insufficient in number, the computer program will no longer be able to generalize, but will memorize these data, similar to a computer program that does not features Artificial Intelligence. It is also the case of fraudulent transactions, which are present in a substantially lower number compared to legal ones (Pozzolo, Boracchi, Caelen, Alippi, & Bontempi, 2017; Taha & Malebary, 2020). By installing a malicious computer program that reads all stored fraud cases, the perpetrator could create a new and different transaction method, thus committing the fraud crime without being detected by the system. Among the solutions that can be thought of to improve this system would be to reduce the data with legitimate transactions and to increase, even artificially, the cases of fraud to improve the detection process. However, the author could illicitly introduce a data set that would disrupt the AI algorithm, so the criminal risk is not removed by using AI. The above examples support the idea that, currently, there is an intersection between the crime of computer fraud and Artificial Intelligence, given that these neural networks are computer programs that automatically process computer data within computer systems. A problematic perspective exists in relation to the evolution of Artificial Intelligence systems. This technology has been able to "transform" entities that we previously viewed skeptically as computer systems, such as vehicles. Without a doubt, Autonomous Vehicles are true computer systems, which can even commit crimes (Stoica V.). Unlike traditional computer systems, which are simple tools in the hand of a user, systems operating on the basis of Artificial Intelligence gradually begin to lose this character. Taking the example of the humanoid robot Sofia (Retto, 2017), who became a citizen of Saudi Arabia in 2017, the distinction between the crime of computer fraud and fraud committed to its detriment becomes problematic. In a decision on the resolution of some legal issues in criminal matters (Stoica V.), the High Court of Cassation and Justice held that "[t]he difference between the crime of deception and the crime of computer

fraud stems from the fact that, while computer fraud is committed on a computer system, the fraud committed [...] by placing fictitious ads that resulted in damage, takes place through a computer system in which computer data is entered (the fictitious ad), resulting in inappropriate data the truth, in order to be used in order to produce a legal consequence, i.e. to create a prejudice to the subject who accepts the fictitious offer. In the case of the crime of computer fraud, the damage is caused as a direct consequence of the introduction of computer data, and in the case of the crime of deception, the damage is caused by causing the injured person to adopt a harmful conduct". By the same decision, it was also held that "while the computer fraud is committed on a computer system, the structure of which is modified, the deception by placing fictitious ads that resulted in damage takes place through a computer system, a whose structure is used by the active subject of the crime". Therefore, the distinction between the crime of deception (art. 244 Criminal Code) and the crime of computer fraud (art. 249 Criminal Code) is made according to the criterion of the "subject" misled: if the misrepresentation operates against a person we are talking about the crime of deception, on the other hand, if the computer system is acted upon, is the crime of computer fraud, an aspect also confirmed by the specialized literature31. If at this point, we can formulate with certainty the conclusion that misleading this robot in order to obtain a material benefit constitutes the crime of computer fraud, as such systems with Artificial Intelligence acquire an increasingly autonomous character from a programmer or user, the legal framework will no longer be so easy to perform. This is because, finally, with the transition from specialized to general Artificial Intelligence, the latter having its own consciousness and a human-like behavior, the question arises to what extent it still constitutes a computer system or program. I believe that there will be reluctance to retain the offense of deception in this case, given that such an entity would still meet the statutory conditions to be included in the category of computer systems that data, but the solution may equally depend of the acceptance of the concept of "legal personality" in the matter of Artificial Intelligence, because only in this case the determination of the injured person to adopt a harmful conduct could be analyzed in the scope of the crime of fraud.

3. Computer Fraud in the Analysis of the European Union

From the contents of par. 86 and 87 of the Explanatory Report, the conclusion can be drawn that the essence of the crime of computer fraud is the manipulation of

computer data - art. 8 lit. a) from the Convention, or manipulation of an IT system - art. 8 lit. b) from the Convention.

The notion of computer data manipulation consists, within the meaning of the Convention, in an intentional act, committed without right, which results in patrimonial damage, and which involves any introduction, alteration, deletion or suppression of computer data. Also, the notion of manipulation of an IT system consists of an intentional act, committed without right, which results in patrimonial damage, and which affects, in any way, the functioning of an IT system.

Therefore, the two alternative forms of the crime of computer fraud provided by art. 8 lit. a) and b) of the Convention, do not necessarily imply a financial transaction, a payment or any other type of commercial operation carried out through computer systems, but it also does not exclude the possibility that through the act of the author to manipulate computer data or the computer system, to produce one of these results, which means that crimes whose material element is the performance of such operations (such as the offense provided for by art. 250 of the Criminal Code – fraudulent financial operations), do not automatically exclude the detention the crime of computer fraud.

Therefore, considering the description of the facts that would fall under the scope of computer fraud, from the perspective of the Convention, it can be said that unlike crimes aimed at carrying out financial operations, or other commercial operations through computer systems, the crime of computer fraud, in the first alternative form of incrimination, it has as its material object the very data that is acted upon in the ways provided by the incrimination text (introduction, alteration, deletion or suppression), to the extent that these data can be considered intangible movable assets with economic value (Stoica V.). In this type of crime (provided by art. 8 letter a of the Convention), the character of intangible movable property is essential, compared to the condition imposed by the incriminating text regarding the occurrence of patrimonial damage. If the data that is acted upon in the ways shown do not have an economic value, so they cannot be included in the category of intangible movable assets, I consider that the crime of computer fraud cannot be retained, because one of the elements of typicality would be missing.

From this perspective, the distinction between the crime of computer fraud and crimes involving the performance of financial or commercial operations through computer systems becomes even clearer, considering the fact that the owners of the two social values can be different persons or entities. It is obvious that computer data as intangible assets can belong to or be managed by the entity that manages the

computer system, while the sums of money or the values represented (at a logical level) by these computer data can belong to other people (actually those several times they belong to other persons or entities), respectively of those who benefit from the services offered by the entity that administers the IT system.

Specifically, resorting to a very simple example, it is obvious that a sum of money transferred fraudulently from a person's account, through unauthorized access to a bank's server, belongs to the account holder (respectively to the client of the bank who benefits from banking services), while the computer data through which this amount of money is logically represented, data managed on the bank's server and which are altered, modified or deleted by the same action that resulted in the transfer of the amount of money, belong to the bank, as the owner of the server but also of the data stored on it, data which through the value of the services provided by the bank acquire the character of goods intangible assets.

In the example given, it can only be a single crime in the situation where the author acted by impersonating the account holder from which he transferred the amount of money, that is, he used the service offered by the bank on behalf of the account holder, without his consent. If, however, the author acted directly on the computer data stored on the bank's server, without using the identification data of the account holder, but the result of his actions was the transfer of that amount of money, it seems that we are in the presence of both crimes, causing harm both patrimonial values protected by the two crimes (the patrimonial value of the IT data as intangible movable assets, or of the IT system whose operation was affected - which belong to the bank; as well as the nominal value of the amount of money transferred - which belongs to the account holder) .

One can easily imagine a situation in which the author is paid by a third party (for example, a competitor of the IT service provider targeted by the author), in order to manipulate the data or the IT system in the IT service provider's possession or administration. In this situation, through the manipulation of the computer system by the author, the damage is produced in the patrimony of the service provider and consists of an economic damage materialized in affecting the services provided by him and implicitly in the decrease of their commercial value, and the material benefit sought by the author consists in the amount of money promised to him by the third party.

An additional argument to conclude that the crime of computer fraud has an autonomous character compared to the other crimes related to carrying out financial

transactions or other commercial operations through computer systems, is the very evolution of European norms in this matter.

Relevant under this aspect, after the ratification by Romania of the 2001 Convention on computer crime, through Law no. 64/2004, the Council of the European Union adopted the Framework Decision 2005/222/JAI/24-feb-2005, regarding attacks against computer systems, this being later replaced by Directive 2013/40/UE/12-aug-2013, regarding attacks against computer systems.

In both acts, the norm of criminalizing the crime of computer fraud from the 2001 Convention on computer crime is practically resumed (art. 4 and 5 of Directive 2013/40/EU and respectively art. 3 and 4 of Framework Decision 2005/222/JAI), and the content of both acts shows the clear intention of the EU legislator to establish rules for the prevention and combating of acts aimed at computer systems and implicitly the computer data processed/stored through them, without making any reference to financial transactions or to any other commercial operations carried out through these computer systems.

Both modalities of the crime of computer fraud provided for by art. 8 lit. a) and b) from the Convention (respectively the frauds that target computer data, or those that target the operation of the computer system) were taken over in art. 249 Criminal Code, article of law included in Title II of the special part - crimes against patrimony, in Chapter IV - fraud committed by computer means and electronic means of payment.

Therefore, the autonomy of the crime of computer fraud is given, among other things, by the legal object concerned, i.e. by the protected social value, which is different than in the case of crimes involving financial transactions or any other commercial operations, through computer systems.

4. The Incrimination of Computer Fraud in Romania

From this perspective, I consider that the name of the chapter of the Criminal Code in which the offense provided for by art. 249 of the Criminal Code is inaccurate, precisely in consideration of what has been shown, in the sense that the crimes it includes do not only cover fraud committed through computer systems and electronic means of payment, but also fraud committed on or against computer systems, at least in terms of the crime of computer fraud.

An interesting problem that the judicial practice will have to solve is the establishment of the legal framework of the act of the author who uses in bad faith a tool for accessing data made available by an economic agent (seen as an IT service provider), a tool made available to him by the administrator of the IT system and IT data (any kind of software application or any other kind of hardware device which falls into the category of computer systems), and through his action, the author performs a manipulation of computer data or computer systems within the meaning of the crime of computer fraud, provided for by art. 8 lit. a) and b) of the Convention, and taken over by art. 249 Criminal Code. (Stoica V.).

We can imagine the situation in which the user of an online library, using his own access data to the computer system (e.g.: his own user and password) and acting under a real identity but in bad faith, would succeed strictly using the web interface, or the applications made available by the library, to enter, transmit, modify or delete computer data, to restrict the access of other users to the library data, or to prevent in any way the operation of the computer system on which the library data is located, in the sense of the provisions of art. 249 Criminal Code.

The question that arises is whether under the conditions in which, acting in the manner described above, the author's aim would be to obtain a material benefit for himself or for another (he could act, for example, for the purpose of appropriating some borrowed books), and his actions would have caused damage to the library (the damage could consist of both the value of the books wrongfully appropriated by the author and the damage to the services offered by the library to other users), the author would be liable for the offense provided for in art. 249 Criminal Code? (Bulancea, Zlati, & Slăvoiu, 2017)

In other words, we are in the presence of the crime of computer fraud, provided by art. 249 of the Criminal Code, in situations where, through the author's act, there is damage to the property of the injured person, the author's goal is to obtain a material benefit, but does he act strictly by means made available by the administrator of the data and the IT system?

At first glance, although at least apparently, all the typical elements of the offense provided for by art. 249 of the Criminal Code, I think there would be serious difficulties in apprehending the commission of the crime.

On the one hand, since the author acted strictly through the means made available by the data administrator, it would be particularly difficult to prove that he acted in bad faith and with the intention of causing damage to the IT service provider's

patrimony. On the other hand, it would be at least unfair to penalize a user of the IT services made available to him, for the lack of diligence of the provider of these services in taking minimal security and data protection measures and the IT system.

In the case of the crime of computer fraud provided for by art. 249 of the Criminal Code, unlike the offense of fraudulent financial transactions, provided for by art. 250 Criminal Code, the author can use any kind of means. The way in which he manipulates the data or the computer system, in the case of computer fraud, can be, at least in principle, an application made available by the administrator of the data concerned, an application that the author uses fraudulently, or it can be any other means his computer (computer program written by the author or procured by him for the purpose of manipulating computer data), means by which he can act on the computer data, bypassing the protection and security systems of the data administrator. (Forbes)

As a consequence, it can be considered that whenever the author uses a service made available by the entity that administers the computer data, data that at a logical level represent monetary funds (electronic currency) or virtual currency (this service materializing in any instrument of payment without cash – bank card, online trading application, electronic wallet, etc.), we are dealing with the offense provided for by art. 250 Criminal Code, and from this perspective (only from this), the crime of fraudulent financial operations has a special character compared to the crime of computer fraud.

In the situation where, on the contrary, the author does not use any service (implemented by the use of a software application or hardware equipment) made available to users for accessing or using the data, the condition provided by art. 250 of the Criminal Code (on the use of a non-cash payment instrument), I believe that we are in the presence of the crime of computer fraud provided for by art. 249 Criminal Code, even if the computer data on which the action is taken logically represent monetary funds (electronic currency) or virtual currency, and the result of the author's action can be assimilated to a " financial operations" in a broad sense (transfer of assets from one holder to another).

In other words, if the author uses the internet banking application made available by the bank, by impersonating the account holder's identity, the offense of fraudulent financial operations, provided for by art. 250 para. 1 Criminal Code. On the contrary, if the same author will act on the same data administered by the bank (by directly modifying the computer data that logically represents the balance values of some accounts - for example), and his activity will have the same result as if he used the

internet banking application (for example, it would operate a modification of computer data in the sense of debiting a user's account and crediting his or another person's account with the same monetary value), we will be (and or only?) in the presence of the crime of computer fraud, provided by art. 249 Criminal Code.

This distinction is all the more important as it constitutes a determining criterion in the identification of the passive subject of the crime, with direct effects on the criterion of identification of the patrimony in which a damage occurred within the meaning of the provisions of art. 249 Criminal Code.

4. Conclusions

The hypothesis presented is only a starting point for the evolution of the ways of committing the crime of computer fraud. Artificial Intelligence is a field that is currently predominantly relevant in the preventive side of criminal law, but it must also be studied in the context of the development of the ways of committing the crime of computer fraud. It is up to the doctrine and jurisprudence to adapt to this evolution and to find effective solutions in order to solve the cases having as their object the sphere of computer crime in general, respectively the crime of computer fraud in particular.

Bibliography

Alpaydın, E. (2014). *Introduction to Machine Learning, 2nd ed.* Cambridge: The MIT Press: .

Bulancea, M., Zlati, G., & Slăvoiu, R. (2017). Codul de procedură penală. Comentariu pe articole/Criminal Procedure Code. Commentary on articles, ed. II. In M. Udroiu. Bucharest: C.H. Beck.

Forbes, ,. l. (n.d.). Retrieved 08 08, 2024, from https://www.forbes.com/sites/meriameberboucha/2018/05/28/uber-selfdriving-car-crash-what-really-happened/?sh=2cff24264dc4

Husti, G. (2021). Acțiunea, inacțiunea și legătura de cauzalitate în cazul inteligenței artificiale/Action, Omission and Causality Regarding. *Temis, no 1-2*.

Malik, E., Khaw, K., Belaton, B., Wong, W., & Chew, X. (2022). Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. *Mathematics, 10, 1480*. Retrieved 08 12, 2024, from https://doi.org/10.3390/math10091480

Matthias, A. (2018). *Neural Networks without the Math, Joyful AI, Book 1*. Joyously Aware Media.

(n.d.). *OECD Recommendation on Artificial Intelligence.* Retrieved 08 10, 2024, from https://www.oecd.org/science/forty-two-countries-adoptnew-oecd-principles-on-artificial-intelligence.htm

Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). IEEE Trans. Neural Netw. *Learn. Syst., vol. 29, no. 8*, 3784.

(n.d.). *Proposal for a Regulation of the Parliament and the Council on Artificial Intelligence.* Retrieved 08 11, 2024, from https://ec.europa.eu/

Retto, J. S. (2017). *First Citizen Robot of the World.* Retrieved 08 09, 2024, from http://bitly.ws/xQvB

Stănescu, C. (2021). *Crearea de portrete fictive utilizând rețele neurale adversariale. Relația cu infracțiunile de fals/ Creating fictional portraits using adversarial neural networks. The relationship with the crimes of forgery.* AUBD - Legal Forum, no 3. Retrieved from https://www.universuljuridic.ro/crearea-de-portrete-fictive-utilizand-retele-neurale-adversariale-relatia-cu-infractiunile-de-fals/

Stoica, V. (n.d.). *The notion of intangible property in Romanian civil law.* Retrieved 08 10, 2024, from https://www.juridice.ro/essentials/1646/notiunea-de-bun-incorporal-in-dreptul-civil-roman

Taha, A., & Malebary, S. (2020). ntelligent Approach to Credit Card Fraud Detection Using an OLightGBMI. *IEEE Access, 8*, 25579.

Zlati, G. (2020). *Tratat de criminalitate informatică/ Treaty on Computer Crime. Vol. I.* Cluj: Ed. Solomon.