Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 9 (58) No. 1 - 2016

THE VIRTUAL THEFT AND THE ILLEGAL USE OF A COMMUNICATION TERMINAL

Adrian C. MANEA[1]

Abstract: *The crimes characteristic to the cyber world are a serious criminal phenomenon due to the ease in camouflaging the offense, but also the cross-border character through the Internet environment.*
The interest to criminalize the offenses committed by computer means, as well as the offenses committed on information systems is justified in the contemporary society by the unprecedented development of information technologies that extend gradually in all fields, from industry to medicine, from e-commerce and internet banking to data management platforms used by the administrations and public institutions.
The paper addresses the issue of criminalizing the illegal use of a communications terminal as a prerequisite for committing cyber crimes.

Key words: *communication terminal, network, Internet, Wi-Fi.*

1. Introduction

In the current regulation of the Criminal Code, cybercrimes have two distinct sections devoted, grouped depending on the social value protected by the incrimination, respectively the fraud committed through computer systems and means of electronic payment, grouped as crimes against property in Title II Chapter IV (article 249 – article 252) of the Criminal Code, namely the offenses against the security and integrity of information systems and data grouped as crimes against the public security in Title VII Chapter VI (article 360 to article 366) of the Criminal Code.

The offenses committed against or using computer systems were previously regulated in two specific criminal laws, namely Law No. 365/2002 on electronic commerce and Law No. 161/2003 on measures to ensure the transparency in the exercise of public dignities, public functions and in the business environment, the prevention and punishment of corruption.

[1] Transilvania University of Braşov, a.c.manea@unitbv.ro

Given the mobile asset character of the computer system, as defined in article 181 of the Criminal Code, respectively any device or group of interconnected or related devices, one or more of them ensuring the automatic processing of data, using a computer program, the actions through which the computer systems are illegally accessed in order to obtain information data, the integrity of the information data stored in such a system altered or with the purpose of disrupting the operation of the computer system are criminalized in the chapter regarding offenses against the security and integrity computer data and systems being found in article 360 - article 366 of the Criminal Code.

Through this type of deeds, the offender intervenes on the information system from the outside, interconnecting to the devices of the computer system either directly, physically, or indirectly via the Internet.

Thus integrating in the computer system, the deeds are committed directly on the computer system, most often hiding originally under the form of system errors, the system administrator identifying the intruder later on.

Being a determined movable in material form, the computer system may become the material subject of other types of crimes and here we consider theft (article 228, article 229 Criminal Code) respectively destruction (article 253-255 Criminal Code), thus being protected from theft or physical damage by the general regulation of the two crimes, when the material element consists of the author's appropriation without being entitled to, of the information system or damaging, degrading or rendering the disuse of a computer system regardless of the aim pursued by the author.

Starting from the way information and data are disseminated in a computer system, respectively from one computer system to another through the Internet and Intranet networks and the way computer networks are interconnected in the virtual environment, the offense regulated by article 230 paragraph 2 of the criminal Code - theft with the purpose of using somebody else's communication terminal or using a communication terminal connected to a network without having the right is regulated as a form of theft for the purpose of use as the current IT technologies enable the connection of a computer system or device to the network used by another system and thus illegally accessing the latter.

Although the Romanian legislature has placed this indictment in the general regulation of the theft, respectively as a form of theft for purposes of use, the phrase theft for purposes of use of a communication terminal being used for the first time in the current content of the Penal Code.

In the current context of an information society and expanding use of information systems in all domains, we consider appropriate the redrafting of a text in the Criminal Code on cybertheft, having as a specific form the illegal use of somebody else's communication terminal or using a communications terminal connected without the right to a network, this material being due to bring technical and legal arguments in this respect.

2. Technical and Legal Arguments on the Opportunity of Distinctly Criminalizing the Cybertheft

With reference to the practical situations in today's society concerning the unlawful appropriation of some forms of energy propagated through waves or energy or magnetic streams, respectively throwaway programs in analog or digital format, such as the theft of electricity or TV signal theft, cybertheft can be equated with the TV signal theft and should be criminalized explicitly and distinctly as a crime through which the virtual environment is protected in general, in order to end the legal controversies in the doctrine regarding the content of the phrase energy with economic value, also used in the current text of the Criminal Code - article 228 paragraph 3 to assimilate certain categories of energy to movable material assets constituting the crime of theft.

In the evolution of criminal regulations in the Romanian codes, we notice that compared to the old Penal Code, the current regulation of the movable concept through the assimilation brought by article 228 paragraph 3, the final sentence, the assimilation of electricity to the movable notion referred to as such is expressly distinguishable, and also by analogy to any other kind of energy that has economic value.

Thus, assimilating to movables all types of energy, be it electric or magnetic, the legislator introduces as an element of distinction the economic value englobed in that type of energy, without distinguishing from a technical point of view between issuing or spreading the respective energy into the environment.

Because of the economic value found in the energy stolen through theft, a real, definable and concrete prejudice is caused to the injured party, the offender's purpose being to evade the obligation to pay the economic value of the energy acquired in this manner.

Not even the TV signal theft from the cable networks is covered expressly by the current Criminal Code as a specific offense, in order to protect the financial interests of the subscribers from different providers of TV programs and implicitly the providers of TV programs that are prejudiced in this manner by those who evade paying the monthly subscription with the equivalent value of the subscription for these services.

The courts hearing of deeds by which the defendants, using improvisations (from the simplest forms - stranded cables / wires to more complex improvised devices) intended stealing TV signal from the distribution box legally installed by the TV programs provider up to their own property, they have sanctioned such deeds as energy theft with an economic value assimilated to movables under the provisions of paragraph 2 of the criminal Code article 208 related to article 208 paragraph 1 of the Criminal Code by applying article 41 paragraph 2 of the Criminal Code under the old Penal Code texts, respectively article 228 paragraph 3 in relation to article 228 paragraph 1 by applying article 35, paragraph 1 in the form of the texts from the current Penal Code.

Thus, the practice of courts has sanctioned and still does the TV signal theft in the majority of cases, even in the absence of a text criminalizing the offence expressly as is the case of electricity, although there are certain trial courts deciding the acquittal of those

accused of TV signal theft, motivated by the court on the one hand through the lack of a text expressly incriminating the offense, or technical reasons in the sense that the TV signal targets the electromagnetic energy, and this has no economic value on its own, which resulted from the fact that the signal cannot be quantified, measured, and on the other hand considering that the damage alleged by the civil party (TV provider) arises only from the service contract, as a result of violating its provisions thereof, thus being on the realm of contractual illicit and civil liability - penal sentence. no. 6087 of 16.12.2003, Court- Targu Jiu (2003, December 12).

Although the solution of Targu Jiu Court was also maintained on appeal by the Gorj Court, Craiova Court of Appeal has made the legal classification of offences on the provisions of article 208 paragraph 2 related to article 208 paragraph 1 of the old Penal Code, applying article 41 paragraph 2 of the Criminal Code, ruling by Decision no. 930 / 07.07.2004 retaining judiciously that SUCC colour video signal represents an electromagnetic energy that can be measured, the unit used being MHz, and in the light of provisions of article 208 old paragraph 2 of the Criminal Code, this energy has economic value determined mainly by the expenditures for capturing, processing and relaying the signal, for which the plaintiff, respectively the TV provider was prejudiced by the lack of the monthly subscription that should be paid to the company, a subscription to cover the company's expenditure with the raw material and the personnel required in order to cable service delivery, namely the expenditure on copyright payments and taxes for cable, fibre or satellite retransmission of the TV programs (2004, July 7).

Discussions regarding not integrating the TV signal or phone pulse in the category of the energies with economic value assimilated to movables, intangible, without a noticeable material existence, have been present in the literature since the adoption of the Criminal Code during the time of Carol II.

Afterwards, the Romanian lawmaker from 1968 criminalized the theft of electricity from the supply networks, even though we are in the presence of an intangible asset, not susceptible of being stolen, considering the economic value attributed to electricity in conjunction with the ownership on the electricity from the network and the costs for producing, storing and transmitting the electricity through the network to the users who pay the equivalent value for these services.

Thus, the Criminal Code "Carol II" expressly provided for in article 524, paragraph 2 that: it is considered movable any energy that has an economic value, a wording afterwards taken over in the Code of 1968, article 208 paragraph 2.

Amid the doctrinal discussions but also the evolution of technologies and identification of other types of energy incorporating economic value, not having a material form, the current regulation of article 228 paragraph 3 of the Criminal Code clearly distinguishes electricity from other energies assimilated to movables likely to be stolen.

Lawyers opposing the inclusion of these types of energy, including electricity, within the movables assimilated go strictly on a legal interpretation regarding the impossibility of stealing goods that have no consistency, the essence of theft / ownership / possession being the physical presence of the asset in the hands of the perpetrator.

And not only the Romanian criminal doctrine has faced contradictory interpretations regarding the assimilation of the fraudulent energy theft from another person's heritage to theft, such discussions being present in the French and Italian doctrine (2016 LegeAZ.net),.

Although similar to the Romanian penal system, the penal codes of the two countries either assimilate energy to a movable (article 624 Italian Penal Code) or expressly provides that the fraudulent stealing of energy from another heritage is assimilated to theft (article 311 - article 312 C.pen.fr.).

Yet the wording in article 228 paragraph 3 of the Criminal Code is too general and susceptible of interpretations as those mentioned above regarding the cybertheft, given the fact that information and computer data moving between different systems in the virtual environment are stolen through the illegal access to Internet network, because we would be in the same situation of an intangible object, but with virtual materiality and which is associated a different economic value, depending on the area to which the information belongs.

In today's information society, in the cyberworld, information and data circulate over the Internet, having their own economic value, from the industrial field in the medical one, from education to banking and financial transactions are made, from procurement of goods and services to electronic payments, all these operations being greatly simplified and accelerated through the use of computer systems connected in networks for computer data transmission, especially in case of cross border operations.

On this virtual route cybercriminals intervene, who, connecting to the Internet, and especially on Wi-Fi, steal information deflecting it from the original route or appropriate it using false identities (IP).

Investing the information and computer data in the cyberworld the nature of energy, and thus implicitly equating the cyberworld with economic value in itself or associated to a material movable, likely to be the subject of acts of theft / taking / appropriation / possession, we consider it appropriate to criminalize cybertheft under the same conditions as the theft of any movable.

In this regard we agree with the technical legal argument regarding the existence of cybertheft, endorsed in his PhD thesis by Florin Encescu (Encescu, 2010: 13), the ability to monetize through taking possession of the virtual goods. Although the virtual environment seems immeasurable, taking possession of the virtual goods / information is limited by moving the goods from the place where the user expects them to be in another virtual place and preventing the legal user to access the virtual goods or making it impossible to use them, even if visible .

Tracking and finding the goods in the virtual environment should not pose problems in theory, proceeding to the identification of the traces in the computer system, the encryption keys used and the accounts accessed illegally.

3. Stealing the Use of a Communication Terminal

Taking from the old Criminal Code of 1968 the incrimination of stealing the use of a vehicle as a form of theft (article 208 paragraph 4 of the old Criminal Code), the current general criminal law incriminates distinctly the theft with the purpose of use in article 230 and identifies two different situations in terms of the material object, but penalized in the same terms as theft and aggravated theft, where appropriate, with special limits reduced by a third.

Neither the wording in article 230 paragraph 2 of the Criminal Code regarding the variant of theft in the form of using without permission a communication terminal belonging to somebody else or using a communication terminal connected to a network without having the right, if a prejudice was caused, is exempt from interpretations and controversial doctrinal discussions, caused primarily by the lack of definition in the Criminal Code of the concept of *communication terminal,* by comparison with the definitions contained in article 181 of the Criminal Code regarding the information system.

This legislative gap can be complemented taking into account the characterization of a communication terminal as an information system, based on the capacity of the communication terminal to be connected to a network, computer network to which information systems usually connect.

And if the legislature did not define the concept of communication terminal, the IT experts aren't convinced either that the text aims at criminalizing the concept of terminal and Wi-Fi access point (Manolea, 2009, September 29), while the Wi-Fi access point isn't a device or an information system, because when connecting to a Wi-Fi point of access, the terminal will be represented by the computer or phone thus connected by accessing the protection password in case of a protected Wi-Fi access point, namely by identifying the router in case of the unprotected or public networks.

Another specialist and author of works in the field of cybercrime, Maxim Dobrinoiu, claimed at the time the New Penal Code was published that the incrimination in article 230 paragraph 2 of the Criminal Code refers to connecting a device without right to the Wi-Fi signal by using applications to crack the password of the protected access point or by some settings of the operating system of the intruder device, when connecting illegally doesn't aim at accessing files or router settings, respectively linking with the other components of the system.

By accessing fraudulently the Wi-Fi signal, as described above, we have the objective side of the crime of theft by using illegally somebody else's communication terminal in order to circumvent the payment of fees to access Internet services to the authorized providers by using the Internet network through another user's router (Dobrinoiu, 2009, p. 12).

In this way, the computer data contained in the electromagnetic emission (broadcast radio) carrier of the Internet signal, although public in the virtual environment, is used

illegally by the users accessing without permission the Internet via an IP router of a user / owner / holder who has purchased the Internet services from an Internet service provider (ISP) in return for a subscription for a database, dealing with a theft for purposes of use as regulated by article 230 paragraph 2 of the Criminal Code.

However, if accessing the Internet is not the purpose of the unauthorized user, but the Wi-Fi network itself is pursued by accessing the Wi-Fi network and implicitly the information systems interconnected to this network, or accessing the Wi-Fi access point is pursued as a way of accessing the computer system of the local network, clear evidence existing regarding accessing the settings or the files of the router or the intention to interact under a false name with other network components (computers, phones, pads, etc.) then the legislative incrimination is article 360 Criminal Code - the illegal access to a computer system. In the latter situation, the Wi-Fi access point is assimilated to a computer system itself, protected by the rule in article 360 Criminal Code.

With the expansion of Wi-Fi networks and their use for commercial purposes by a company that provides hotspot services, such as a restaurant or a hotel that offers those Internet access services for free to its customers, respectively to the customers who eat or drink in the respective location, a dilemma that appears and is practically labelled in IT terms piggybacking, is whether the people outside the business location that manage the Wi-Fi network and also access the network fraudulently, because they do not provide a counter service to the company concerned, are liable to be sanctioned for the offense of theft for purposes of use, especially where the access to the Wi-Fi network, either by ignorance or negligence, is not protected by password, being basically a private Wi-Fi network with public access.

4. Conclusions

Compared to the current regulation of the Criminal Code by including the criminalization of illegally using somebody else's communication terminal or using a communication terminal connected illegally to a network as theft for purposes of use in article 230 paragraph 2, distinctly criminalizing the illegal access to a computer system (article 360 Criminal Code), we consider that great steps have been made in the field of cybercrime, somehow establishing the criminalization of cybertheft, as a distinct form of theft in the simple form (article 228 criminal Code) and aggravated form (article 229 Criminal Code).

At the same time by introducing the text of article 230 par.2 Criminal Code, legal progress has been made in terms of the classifying electromagnetic emission containing computerized database in the content of the concept of *energy that has economic value* according to article 228 paragraph 3 Penal Code, respectively assimilating the electromagnetic emission to an incorporable movable.

References

Dobrinoiu, M. (2009). Provocarea legislativă a rețelelor Wi-Fi [The legislative challenge of the Wi-Fi networks]. *Intelligence Magazine*. Bucharest: Anul IV, no.16, July. Available at: http://e-crime.ro/ecrime/site/index.php/article/. Accessed: 02-04-2016.

Encescu, F. (2010). *Criminalitatea informatică*. Teză de doctorat [Cybercrime. Thesis]. – Nicolae Titulescu Bucharest University. Available at: http://www.univnt.ro/rezumate_doctorat/index.php?dir=Drept%2F&download...pdf. Accessed: 22-03-2016.

Manolea, B. (2009). *Infracțiunile informatice din Noul Cod Penal.* [Cybercrime in the new Penal Code]. Available at: http://legi-internet.ro/blogs/index.php/infractiuni-informatice-noul-cod-penal. Accessed: 22-03-2016.

*** *Conectarea ilegală la un serviciu telefonic* [Illegal connection to telephone service] LegeAZ, 2016. Available at: http://legeaz.net/dictionar-juridic/conectare-ilegala-serviciu-telefonic. Accessed: 12-03-2016.

*** Court of Tg-Jiu, *The criminal punishment no. 6087 from 16.12.2003*. Available at: http://www.hamangiu.ro/upload/cuprins_extras/infractiuni-economice-practica-judiciara_extras.pdf. Accessed: 22-03-2016.

*** Court of Appeal from Craiova, *Prosecution Decision no.930/07.07.2004.* Available at: http://www.hamangiu.ro/upload/cuprins_extras/infractiuni-economice-practica-judiciara_extras.pdf. Accessed: 22-03-2016.