ACCESS TO A COMPUTER SYSTEM. BETWEEN LEGAL PROVISIONS AND TECHNICAL REALITY

Maxim DOBRINOIU[*]

Abstract

Nowadays, on a rise of cybersecurity incidents and a very complex IT&C environment, the national legal systems must adapt in order to properly address the new and modern forms of criminality in cyberspace. The illegal access to a computer system remains one of the most important cyber-related crimes due to its popularity but also from the perspective as being a door opened to computer data and sometimes a vehicle for other tech crimes. In the same time, the information society services slightly changed the IT paradigm and represent the new interface between users and systems. Is true that services rely on computer systems, but accessing services goes now beyond the simple accessing computer systems as commonly understood by most of the legislations. The article intends to explain other sides of the access related to computer systems and services, with the purpose to advance possible legal solutions to certain case scenarios.

Keywords: *cybercrime, access to computer system, cyber-attacks, information society services, botnet, email access, point-of-sale, web access, criminal law, offence.*

1. Introduction

In a very complex virtual environment, at the European level, the applicable national legislations on cybercrime are mainly based on the Council of Europe Convention on Cybercrime, concluded in 2001 in Budapest. A good document and a real beacon for law enforcement and judicial systems across Europe (and many other countries) for more than a decade. But we now witness that some of its provisions seem to be far away behind the nowadays technological developments and the actual operation tools and methods used by the criminals in cyberspace.

Some countries understood the need for a more comprehensive legal approach of the new improvements in the criminal cyber-activity, while others still remain bound to the old concepts and try to improvise in the search for the correct solutions in complex cases involving new sort of cyber-attacks and new IT&C means of committing cyber-related crimes.

2. Terms and definitions

The CoE Convention defines the computer system as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

Computer data is regarded as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer to perform a function".

Meanwhile, the service provider means "any public or private entity that provides the users of its service the ability to communicate by means of a computer system", as well as "any other entity that processes or stores computer data on behalf of such communication service or users of such service".

Sometimes, mistakes are made in the understanding computer programs and data as indispensable parts of computer systems, and thus, people wrongfully regards the user's interaction with them as an interaction (see access) with computer systems. For example, a simple interaction with an antivirus application installed on a PC cannot be regarded as an access to (entering) the remote antivirus server belonging to a certain IT security company.

3. Access to computer systems versus access to information society services

Acting as a source of inspiration for national legislations, the CoE Convention on Cybercrime provided for, in Article 2, the illegal access to a computer system as "the access to the hole or any part of a computer system without right", while at point 46 of its Explanatory Report, the European legislators came with much deeper conclusion, stating that the access should be seen and interpreted as "entering of the hole or any part of a computer system (hardware, components, stored data of the system installed, traffic and content-related data)".

This understanding provided for national legislations the grounds of incriminating acts like "hacking", "cracking", "computer trespass" or any other operation in which the perpetrator illegally succeeds to "enter" or to "break into" a computer system, either it is a standalone one or a remote workstation connected to a network.

[*] Nicolae Titulescu University, Bucharest (e-mail: **office@e-crime.ro**).

Furthermore, a common agreement concluded that there is no (and shouldn't be) "access to a computer system" in situations like: sending an email message from one computer system to another or file transfers between systems.

The meaning of "enter", "break into", "hack into" and likewise terms is that of the creation of a direct and continuous virtual liaison between an individual and a machine, of a nature that allows the individual to treat the computer system almost like a physical location (ex. a house), having the possibility to perform different actions while inside (ex. turning the light on/off, resting on a sofa, opening the fridge in search for food, using the toilet etc.).

Once this direct link is somehow disconnected (irrespective whether it is resumed in the future) the virtual presence of the individual into the machine is over and is quite similar to getting out or leaving the "house".

Over time, either by interpreting the CoE Convention on Cybercrime (and its Explanatory Report) or creating their own provisions, national legislations preferred the term of "access to" in order to identify and further prosecute certain interactions between individuals and computer systems. But, in reality, taking into consideration the above mentioned considerations and the technical ways such interactions occur, one could notice that just few of the real situations are properly covered by the legal articles involving the "access to" expression, as it could be exampled herewith.

Access to a Computer System

In its simplest way, the access to a computer system (network) requires a direct interaction with the peripherals (keyboard, mouse) in order to launch commands to the Central Processing Unit and make the system work.

Furthermore, using a system's functions and the possibility of processing data could also be regarded as "access" to that system[1], because the interaction and the continuously "logical" liaison between the user and the machine is one of the kinds that creates the conditions for the existence of a virtual presence of that specific user "into" the system.

From a distance, there are multiple possibilities to have an access to a system, especially when, using his own system and specific tools, the user finds a way to (re)create and administer the virtual continuous liaison with the targeted computer (in the same network or in Internet). Is the well-known case of using a Remote Access Tool (or Remote Administration Tool), a software that creates a continuous communication channel between two separate systems, with the possibility for a user to virtually be present in another one's system (with the purpose of performing administration tasks or solving specific issues).

The problem with some of the national legislations is that the "access to computer data" is conditioned by the "access to a computer system", while the real life shows multiple ways to get hold of computer data without actually "enter" or "hack into" a computer system.

In either the situation presented, the key factor for the "access" is the existence of a (direct or remote) continuous communication channel able to provide a virtual presence of a user within a computer system.

A particular instance of the "computer system" is represented by the smartphone or tablet (communication equipments with operating systems). Any unauthorized use of either such terminals may be easily regarded as a crime of "illegal use of a communications terminal equipment" (if available in legislation[2]), in legal conjunction with the crime of "illegal access to a computer system", taking into consideration that the use of the terminal equipment is equivalent with the "entering in" that "system".

Access to a Web resource

Accessing an Internet resource, such as a webpage, may rather be regarded as the obtaining (remotely) of computer data than an access to a computer system (ex. the web-server).

Technically, it is commonly understood that, when requested by a user (upon entering the respective URL), a copy of the targeted remote webpage is being sent by the hosting web-server directly to the user's browser and then showed him on the monitor. All the operations (at physical, network, TCP[3] or application level) are performed without user's acknowledgement or intervention, while the data traffic simply follow the TCP/IP and HTTP[4] protocols.

It is clear that, in this case, the user cannot (and does not) access the remote web-server and he does not actually "enter" the computer system that operates as web-server in searching for the desired webpage content (computer data). It is more a data exchange, during an established bidirectional and sequential communication between user's browser (PC) and the remote web-server.

As a matter of fact, it is a classic act of a transfer of computer data from a computer system. When committed without right, this is a crime prosecuted and punished by the majority of national legislations. Surprisingly, this situation was not

[1] See Section 1 (1) *Unauthorized access to computer material*, in UK Computer Misuse Act of 1990.
[2] See Article 256 Penal Code of Spain, and Article 230(2) Penal Code of Romania.
[3] Transport Control Protocol.
[4] Hyper Terminal Transfer Protocol.

comprised in the CoE Convention on Cybercrime, but there are suspicions that the European drafters thought of it in the context of the "illegal access to a computer system with the intent of obtaining computer data".

As a particular case of accessing a web resource, the situation when the web-servers send and install in users' PCs the so-called "cookie files" (the same time they send to browsers the desired webpages) may also not be considered as an "access to a computer system", because these files cannot ensure a continuous virtual link between a person (ex. webpage owner) and the destination PCs. They are just small scripts (computer programs) that record and track users' online activity on certain webpages and "help" webpage administrators to easily direct them adware or similar content during the next visits (browsing).

Using "cookie files" is merely a subject of an "illegal interception of computer data" (as a form of cyber-surveillance), but is not considered as a crime (by the majority of national legislations), due to the fact that the users' consent over reception, installation and operation of such software is legally expressed by acknowledging the situation clicking a visible alert available on most of the websites.

Access to an E-mail account

This is a very much disputed situation, both in academia and judicial practice.

It is commonly known that an E-mail account is a space allocated on a Mail server for a specific client (user), identified by a unique E-mail address. The authentication methods usually consist of a username and a password.

E-mail, as generic perceived by people, is not a computer system. It is not a computer program either. It is an information society service or, simply, a "publicly available electronic communications service"[5]. Or, a communication performed by electronic means.

According to Article 2 point (h) of the European Directive 58/2002, the electronic mail is "any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient".

From this technical reality, when it is about an "illegal access to an E-mail account" the judicial system must ensure that there exist a crime of "illegal access to a computer system" or just something else.

Irrespective of the tool a person use for interaction with a remote Mail server – through an E-mail client software (computer program) or a Web Mail service (ex. Gmail, Yahoo etc.), the act of sending, receiving or just reading electronic messages is very hard to be considered as an access to a computer system (the Mail server).

In this case, an eventual offender is not entering the remote Mail server, nor breaking into or hacking into that system. The user simply benefits from the functions of that particular system, which are: receiving, sending or storing E-mail messages from, to or on behalf of the legitimate account owner.

Even when an E-mail client software or a Webmail service is used, messages are often sent or received as copies of specific computer data. Data processed inside or outside a network or between multiple networks.

So, it is merely a sequential communication of data, and thus not a continuous virtual relationship (interaction) between the user and the remote machine (the Mail server), and therefore not a real access.

Surprisingly, we do have an access. Not an "access to a computer system", but rather an "access to an electronic communications service" or simply an "access to a computer service". As mentioned before, E-mail is a computer service, and its usage by a person better fits into this context of "access" seen as a possibility to obtain, to benefit from or to effectively use that service.

Access to Cloud Accounts

Cloud Computing is a general term for the delivery of hosted services over Internet[6]. In Cloud Computing, users access software applications remotely through the Internet or other networks via cloud applications service providers[7].

Simply, cloud computing is a service. An information society service available for users (clients) based on certain access credentials. However, those users don't actually "enter" or "get-in" the remote servers, so there is no "access to a computer system". The files the legitimate users are working on are not stored locally, but on remote servers, while the users interact only on electronic copies of those files (that are transferred to local machines for each particular purpose – read, write, modify, delete).

In case of a perpetrator using, without right, a cloud computing-type service, thus obtaining computer data as results (photos, personal information, financial, official, classified or any other type of information), from a criminal law perspective there is merely an "unauthorized transfer of computer data" (computer data is identified and extracted by the attacker), in conjunction (if the case) with a "data interference" (data is altered or suppressed in any way), a "computer-related fraud" (if a loss resulted), a "computer-related forgery" (if a legal consequence was created), etc.

[5] https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/
[6] http://searchcloudcomputing.techtarget.com/definition/cloud-computing
[7] http://www.financialforce.com/resources/what-is-cloud-accounting/

For all that, the existence of a distinct criminal law provision of "illegal access to an electronic communications service / information society service" would be a better legal solution in this scenario, too.

Access to ATM and POS

There is no doubt that an Automated Teller Machine (ATM) is a computer system. In fact, it is a computer linked to a cash dispenser.

When used by a credit card holder in order to take out cash or to perform certain financial transactions, the interaction with this terminal should always be considered as an "access to a computer system". Thus, in the situation of the access to the ATM by a person with a fake (forged, cloned) credit card or by a person with a valid credit card but with no right or consent from the legitimate holder, there will be an offence of "illegal access to a computer system" along with an offence of "unauthorized conducting of financial operations"[8] or "circulating forged electronic payment instruments"[9].

A Point of Sale (PoS) is an electronic device that operates with the purpose of authenticating an electronic payment instrument (credit card) and its holder to the financial computer system in order to validate a transaction (ex. purchase). Being an electronic device interconnected with an electronic payment system, one should consider it as a part of the whole computer system.

Thus, a person who presents a forged card to a PoS or a valid card but with no consent from the legitimate holder may be liable for committing the offence of "illegal access to a computer system" in legal conjunction with the offence of "unauthorized conducting of financial operations". Irrespective if the interaction between the PoS and the valid card is through embedded chip or wireless[10].

Access to Online Banking

This is another misinterpreting of the term "access to a computer system".

It may look pretty much as an access to a computer system when a person logs in and use the online banking facilities, but, again, the technical realities come to reject this solution.

A portal for online banking is primarily a web interface, an electronic communication service or an information society service, provided in certain conditions by a financial institution (a bank) to its clients. The legitimate users may have access to the information on their bank account (balance, credits, list of transactions etc.) or they may perform some bank-specific operations (online transfer of money to other bank accounts, foreign exchange etc.). But in no circumstance, the user (bank client) is "entering" the bank's computer system. He only relies on the specific data the bank is sending to him, via the web interface (portal), based on his online requests. And, as mentioned before, this is just a sequential bi-directional communication of data (like email exchange) and not a continuous virtual communication channel, as required for the existence of an "access to a computer system".

The same rationale applies in the situation of Mobile Banking, an electronic financial service provided by the banks to their clients, with the purpose to be used on mobile phones, in the form of mobile applications. These mobile applications act as the online interface with the (financial) service offered by the bank, and, through them, a user just only communicate (with the meaning of information exchange) with the bank's computer system or network, while not actually accessing ("entering", "hacking-into") that system.

So, in the case of an attacker using without right an online financial service, there should not be an indictment for "illegal access to a computer system", but merely an indictment for "unauthorized use/access of/to an internet society/electronic communications/online financial service" (in a theoretically possible legal connection with the crime of "unauthorized transfer of computer data" from the bank's computer system, and a "computer-related fraud").

Access to Wi-Fi Hotspots

Different approaches have been recorded, either in academic studies or practical cases, related to the situation of an electronic device (ex. smartphone or a laptop) connected to a Wi-Fi Hotspot in order to get connected to Internet. The legal solutions offered by specialists and authors varied from "illegal access to a computer system" to "illegal interception of data" or simply "theft".

From a technical point of view, a Wi-Fi Hotspot (or Access Point) is a real computer system, because it fits the definition provided by CoE Convention on Cybercrime and numerous national legislations. But the attention of an individual is not focused on the device itself, but on the electronic signals broadcast by the router, carrying TCP/IP packets of data, allowing the connection to Internet. Irrespective if the signal is unencrypted or encrypted with WEP, WPA or WPA2 PSK.

For this reason, this type of wireless connection (to Internet) eliminates the legal possibility of incrimination based on the provision of "illegal access to a computer system" and even on the provision of "illegal interception of data".

In this particular case a possible legal solution would be the incrimination of "the connection

[8] See Article 250 of the Romanian Criminal Code.
[9] See Article 313 of the Romanian Criminal Code.
[10] See PayWave provided by VISA.

without right to a network", with good results in prosecuting the unauthorized access to Internet through Wi-Fi Hotspots.

Access to Computer System through Malware

Hourly, computers and networks from around the world are infected, directly or remotely, with malware. This malware reaches targeted computers via multiple ways of propagation: external storage devices, infected E-mail attachments, infected websites (see Watering Hole Attack), P2P connections, File Transfer operations etc.

The most common infections are Viruses, Worms, Trojans, or Keyloggers. Most of them have a disruptive program to run in order to alter, modify or delete computer data on host system or to affect its good functioning. Some of them are just creating backdoors to perform further actions against the host or to use the host's computing capabilities to launch other virtual operations.

Depending on the design and operation features of such malware, we may have various possibilities of computer-related crimes.

If the malware installed into a computer is of a kind that modify or erase data there should exist the crimes of "data interference" and "system interference".

If the malware operates as a Keylogger, there should only be the generic crimes of "illegal interception of computer data" and "unauthorized transfer of computer data from a computer system".

If the malware contains a software module acting as a RAT[11], there is a crime of "illegal access to a computer system", for the reasons already described.

In Cybercrime and Cybersecurity literature, as well as in real life cases, there were disputes on the opportunity of an indictment of "illegal access to a computer system" in the situation of a Botnet creation.

As commonly defined, a Botnet is a group of computers connected in a coordinated fashion for malicious purposes[12]. Attackers often target unprotected computers and get control over them by infecting with viruses, worms or Trojans. By the use of such collection of "zombie" computers, attacker could further perform multiple Cybercrime specific activities (ID and Data Theft, DDoS[13], Spam, Phishing, etc.). While some of the IT Security specialists may consider that the creation of a Botnet has the technical ingredients for the existence of an "access to a computer system" (taking into consideration the way the Botnet Herder[14] remotely controls and gives instructions to the infected computers), there are also technical arguments that there is no "illegal access to a computer system" on the grounds that a continuous virtual communication channel is missing in the "relationship" between the Botnet Herder and each of the infected machine.

As it is regulated now, in most of the legislations, the "illegal access" ends immediately after the "entrance" of the perpetrator into the target system (directly or remotely), while there are no (or just few) provisions for the rest of the actions the attacker might further perform once "inside" the system.

In this case, a good solution would be the existence of an indictment of "*the access to a computer system that resulted in an unauthorized influence of the function of that computer system*".

Access to Externally Stored Computer Data

Apart from the information stored or processed within a computer system, there are multiple cases when the offenders are looking for computer data stored in external storage means, like Hard Drives, USB Flash Drives, CDs, DVDs, etc.

While most of the national legislations addresses just the obtaining of computer data that is stored, processed or transmitted in/from/to a computer system, almost none provides a solution for the situation data is obtained from a storage mean or device.

Usually, in order to access (see, obtain, process etc.) that electronic data, a user must connect the external storage device to a computer system. His own or another one's, but operated in legitimate conditions. Technically, when such connection occurs, data is temporarily copied into the RAM's host computer in order to further be displayed or available to the user.

Although there is no sign of an "access to a computer system", as defined by the CoE Convention on Cybercrime or the national legislations, there is a "transfer of computer data from a storage device", which, if is performed without right, may result in an offence of "unauthorized transfer of computer data from a storage device"[15].

On the other hand, for a more clear legal situation, *de lege ferenda* should be created a distinct provision incriminating the "unauthorized access to computer data" – as recommended by the CoE Convention on Cybercrime, but not in the general context of the data stored, processed or transmitted in/from/to a computer system, similar to the

[11] Remote Access Tool.
[12] https://www.techopedia.com/definition/384/botnet
[13] Distributed Denial of Service (cyberattack).
[14] The person who controls the Botnet.
[15] See Article 364 of the Romanian Criminal Code – "the unauthorized transfer of computer data from a computer system or a data storage device".

incrimination of the "unauthorized access to online child pornography materials".

4. Final remarks

The above analysis, from both technical and legal perspective, unveils various circumstances where the representatives of the legal sector may wrongly use the criminal charge of "illegal access to a computer system" when the cases actually deal with electronic communications services or information society services.

While still complying to the general recommendations of the CoE Convention on Cybercrime, national legislations should look forward to identifying new and comprehensive legal solutions in order to solve actual controversial situations from real life, and to prepare to properly address (through tough criminal provisions) the new improvements the cybercriminals add to their activity against computer data and computer systems.

Least but not last, national legislations need to focus their criminal provisions on the real impact the electronic communications services already have on the societies, economies and people, creating those solutions that better fit their law enforcement requirements, but from a technical perspective that goes beyond the simple "access to a computer system" way of thinking and interpretation.

Resources:

- Council of Europe Convention on Cybercrime, available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- Explanatory Report on the Convention on Cybercrime, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b
- http://www.cybercrimelaw.net