ID THEFT IN CYBERSPACE

Maxim DOBRINOIU*

Abstract

Obtaining personal data, identification data, including data which allow the use of a electronic payment instrument, or any other data generated in the context of one person's activities in the social, economic or financial life, without its consent or by deceit, if this occurs in computer systems or through electronic means of communications, should be considered as a crime and punished accordingly.

Keywords: *ID Theft, Cybercrime, Social Engineering, Phishing, Computer-related Forgery*

1. Introduction

Like other countries, nowadays Romania need to face, more and more, a exceptionally serious phenomenon, which, unfortunately, haven't got a relevant and comprehensive attention from the legislators.

It is about "Identity Theft" (or ID Theft), with its aggravated form when the action is committed by the use of computer systems or electronic means of communication.

As a notion, the „identity theft" has an improper name, because the identity of a person is not actually stolen, but rather taken over (or assumed, acquired) illegally and further used generally to commit other offences. In other words, we are not dealing with a crime against property, but with a crime against the person (as stated in the New Criminal Code, Title 1, Chapter IX – crimes against the residence and private life of a person).

By „identity theft" one could understand the obtaining, illegally (unauthorized), of personal data or other data related to the social or professional activity of a person or data resulted from the person's interaction with a financial institution, if later on the use of this acquired data is capable to generate legal consequences or to cause a loss of property to that person.

2. Paper Content

From a technical perspective, the „identity theft" could be performed by one of the following methods:

Social Engineering is defined as a collection of means, HW and SW tools and communication strategies by the use of which the victim is deceived related to a situation or a fact and thus manipulated to provide personal data, confidential or financial information, or determined to act in the manner required by the attacker.

The manipulation techniques are used by the attacker in the conversation with the victim (directly, by telephone or through any other electronic mean of communication), while the deceiving is performed with the aim to infringe the victim's psychological „barriers", and make her disclosing data or doing actions that, in other conditions, would have not been done.

* Lecturer, PhD, Faculty of Law, Nicolae Titulescu University of Bucharest (e-mail: office@e-crime.ro).

Pharming is a special type of computer-related attack which takes place when the attacker insert certain computer data in a Domain Name System's IP allocation table responsible with routing the victim's personal computer browser requests to fake webpages or to other internet resources controlled by the attacker.

The Domain Name System (DNS) initiates the process which allow a certain user to connect to a webserver (or a webpage) by typing the desired URL (web address) in the browser address area. It is known that, in Internet, computers communicate only based on IP addresses, and the equipments in charge with the translation of the domain names into IP addresses and back are the DNS servers. These servers store databases with relevant details like <domain name – associated IP address> of the numerous active networks, and have the capacity to memorize new such connections, in order to facilitate the user's fast access to the needed resources. DNS servers are organized on a hierarchical structure, the most important of them (called *root*) being generically named from „A" to „M" and hosted by the significant Internet providers from US, Japan, UK and Sweden.

By methods like DNS ID Spoofing or DNS Cache Poisoning, an attacker has the possibility to modify the DNS allocation table records, and, thus, to redirect the victim's web traffic towards a fake resource or to a server he controls.

Phishing is, maybe, one of the most known crime activity. It is used by the cyber-attackers to steal personal data or identification data related to electronic payment instruments. The victim is lured, often by a convincing email message, to click on a provided hyperconnexion (link) and, through it, to access a fake webpage, imitating almost perfectly the genuine one the user expects to find, hosted on a server controlled by the attacker. Once browsing on the forged webpage, the victim is tricked into providing its personal data, identification data or other kind of information used in financial transactions or online shopping.

Skimming to a ATM is that method by which the perpetrators mount and conceal outside of a cash dispenser (Automated Teller Machine) a device especially designed to read and copy the data stored on the magnetic stripe of the credit cards. While at the ATM, the victim doesn't notice the forged surface (cover) attached and uses its own credit card to perform a certain financial operation. Technically, before the victim's card actually enters into the ATM, its magnetic stripe is read by the microcontroller's head (like reading a videocassette or an audiocassette) and the data is then copied to a storage mean (also concealed in the attacker's equipment). After a variable number of such „read&copy" (depending on the capacity of the storage mean), the attacker comes back to recover the equipment and the masking cover.

Over time, many opinions have been expressed in the criminal doctrine related to the correct indictment of such an action (skimming), but only recently, following an „appeal in the interest of the law" from the Romanian General Prosecutor's Office (the Public Ministry) for the unification of the courts' decisions in this kind of criminal cases, the High Court for Cassation and Justice issued the Decision no. 15 of 14 October 2013, published in the Romanian Official Gazette no. 760 of 6 December 2013, stating that the only applicable legal solution is the one generically called *illegal operations with equipments and computer data*, with the provisions of Article 365 2nd alignment of the new Criminal Code, respectively *the detaining, without right, of a device, a computer program, a password, an access code or other computer data, line those mentioned in paragraph 1, with the aim to commit one of the offences from Articles 360 to 364.*

In this case, the solution issued by the High Court of Cassation and Justice is incomplete, because it doesn't map entirely on the technical reality and ignores the specific link requested by the offence of *illegal operations with equipments or computer programs* (as tool-crime) in connection with another offence (as end-crime or target-crime) which the High

Court fails to nominate in its above-mentioned Decision, but which is obvious and it consists of the crime provided by the Article 364 of the Criminal Code, namely *the unauthorized transfer of computer data from a computer data storage* (the credit card).

In this moment, with the exception of the Skimming (which seems to be in a way solved by the High Court Decision), the „identity theft" is legally regarded as a computer-related forgery (Article 325 of the new Criminal Code), and, in some scenarios when the data has been already used, ID Theft is regarded as a crime against the property or a crime of forgery (the acquiring of personal or financial data being just a preparatory act for those crimes) – which is a false conclusion.

In what regards the computer-related forgery, we find that, in Phishing, the perpetrator actually do realize the specific material acts of the crime provided by Article 325 Criminal Code only on the header of the luring email (the header is modified by *spoofing* in order to trick the victim about the real source of the email) and on the fake webpage (clone). For all that, in order to have an indictment based on Article 325 is strongly necessary that the outcome of the forgery to be able to produce legal consequences.

In the case of email header spoofing (aka *email spoofing*) we could not find any legal consequence, only if the act of taking over another person's identity would occur in dealing with a state authority or an institution among those mentioned in Article 175 Criminal Code. Thus, the legal consequence would be represented by a „identity-related forgery".

Much significant is the legal consequence when faking a webpage, the final place where the victim discloses its personal information. In this case, by cloning the webpage, the perpetrator is guilty of infringing the copyright related to the original (real) webpage, which is the kind of legal consequence requested by Article 325.

In other words, strictly from the perspective of the committed acts, in this very moment, there is no criminal offence to be used against an attacker who, illegally, obtains the computer data related to a person, and seems that this criminal behaviour may be not punishable.

Regarding the activity of the victim while present on the forged webpage, the conclusion is that he/she, misled (tricked, fooled), personally chooses to disclose the information (personal data, financial data, data necessary for the use of an electronic payment instrument and so) „requested" by the attacker. The victim is not constrained in any kind and has the right representation of his/her actions. Misleading (fooling, tricking) is, on one hand, the „fruit" of the attacker's performance as social engineer and as the creator of an almost perfect faked webpage, but, on the other hand, is the result of the lack of education or essential training in security (personal security, computer security etc.) as well as an effect of not knowing or not taking the appropriate security measures the victim knew or had to know.

The victim culpable behaviour related to the protection of its own personal information is not, however, a reason for the Romanian legislator to fail in sanctioning, by not creating an appropriate legal provision, the attacker's overall criminal activity of misleading, luring or manipulating the victim, followed by obtaining, illegally, the data he was looking for.

A *de lege ferenda* proposal could have the following text[1]:

Obtaining personal data, identification data, including data allowing the use of an electronic payment instrument or any kind of data generated by a person's social or economic activity, without its consent or by misleading, if such an action has been performed in computer systems or using electronic means of communication, shall be punished with imprisonment from „x" months to „y" years or a fine.

[1] Similar proposals have been issued in article *Considerations on the Efficiency of the new Criminal Code in Combatting Cybercrime*, Challenges of the Knowledge Society eBook 2013, ISSN 2068-7796, p. 33

Irrespective of the chosen form of criminalisation, shall be absolutely necessary that such a criminal provision exists in a potential future amendment of the Criminal Code.

Is not appropriate, in this context, an amendment to the Law no. 677 of 2001 regarding the protection of personal data, because this legal provision does not regulate the situation when the personal data are processed by an individual (the perpetrator) for its own use and without to be disclosed to third parties.

This analysis only refers to the „essence" of the „identity theft", namely the phase of obtaining, unauthorized, computer data related to a person.

In what regards the electronic storage of the stolen data or the future use (use of identity), these kind of actions are comprised in the materiality of other offences in the Criminal Code, such as: Article 240 – computer fraud, Article 250 – illegal performing of financial operations, Article 251 – the acceptance of illegally performed financial operations, Article 313 – circulating forged values, Article 314 – possession of instruments to perform value forgery, Article 325 – computer-related forgery, as well as Article 365 – illegal operations with equipments or computer programs or Article 388 – the fraud to electronic vote).

3. Conclusion

Taking into consideration that "*nullum crimen sine lege*", the overall conclusion is that the Romanian legislator needs to take, in the near future, certain measures in order to be able to efficiently combat the ID Theft, by creating a comprehensive legal provision, with no or little space for interpretations or different understandings, a real tool for prosecutors and judges. Being a reactive measure, this need to be completed with a proactive one - represented by a Cybersecurity-related awareness campaign, as well as (extra) professional training for all those involved in the prevention, prosecuting, judging or defending in cybercrime cases.

References

- The New Criminal Code of Romania (adopted with modifications by Government Emergency Ordinance no. 3/2014, Law no. 286/2009 and Law no. 187/2012)
- Council of Europe Convention on Cybercrime (Budapest, 2001) and the Explanatory Report
- V. Dobrinoiu and collaborators, *The New Criminal Code Commented*, Universul Juridic Publishing House, 2012, p.725-726