IDENTITY THEFT COMMITTED THROUGH INTERNET

Adrian Cristian MOISE[*]

ABSTRACT: *In this study, starting with the presentation of some aspects regarding management of identity in cyberspace, it is carried out the analysis of the offence of identity theft committed through Internet. The term "identity theft" describes the criminal acts through which the offender obtains and uses in a fraudulent manner the identity of other person. These criminal acts may be carried out through the use of information and communication technology, too. The cases of identity theft committed through Internet have a wide spread, being based on sophisticated frauds, creating difficulties for the law enforcement bodies when they investigate such offences.*
There is no standard definition relating to identity theft. The only element which is found in the definitions regarding identity theft is the fact that it is carried out in several phases, which were extensively analysed in this study. Moreover, in this study are studied the two systematic approaches with a view to incriminating identity theft, existent in the literature: creation of a single provision which incriminates the act of obtaining, possessing and using information regarding identity for criminal purposes; individual incrimination of acts related to obtaining information regarding identity, as well as the acts related to possession and use of such information.

KEY-WORDS: *identity theft; cybercrime; Internet; identity; computer data; cyberspace*.
JEL CODE: *K 14*

1. ASPECTS REGARDING IDENTITY MANAGEMENT IN CYBERSPACE

Identity is a very complex aspect of human nature. One of the most interesting aspects regarding Internet is the chance given to people to present their identity in a variety of ways. There are many factors regarding navigating on Internet, showing how people manage who they are in cyberspace: (Suler, 2002, pg. 455-460)

1.1. Level of dissociation and integration

Due to online groups, each devoted to a distinct professional, vocational and personal topic, people can express, highlight and develop specific interests and life experiences. When people join an online community, they may choose as much information as may be

[*] Postdoctoral Researcher, Titu Maiorescu University of Bucharest, Faculty of Law, ROMANIA
"This work was supported by the strategic grant POSDRU/159/1.5/S/141699, Project ID 141699, co-financed by the European Social Fund within the Sectorial Operational Program Human Resourses Development 2007-2013".

provided to the community they are part of. Online communication tools give people the possibility to choose, if they want to be seen or heard by other people. The desire to remain anonymous reflects the need to eliminate those critical features of their identity that they do not want to display in that particular group.

Cyberspace gives the persons the possibility to develop a certain aspect of who they are. Moreover, cyberspace give people the chance to express and explore facets of their identity, that they do not express in their face-to-face world.

1.2.Positive and negative valence

Human behaviour has two components: a positive one and a negative one. Subjectively, a person can feel shame, guilt, anxiety, or hatred about some aspects of their identity, while accepting and appreciating other aspects. People also strive to attain new, idealized ways of being. People who violate in cyberspace the rights of others are usually discharging some negatively charged aspect of their psyche. An insecure, passive-aggressive person gets stuck in an endless stream of online arguments. Others may use cyberspace as an opportunity to exercise their positive characteristics or to develop new ones in a process of their own behaviour. Some people try to transform the negative feature of their identity into a positive one, or they may change their attitude about that feature.

1.3. Level of fantasy or reality

In some online groups, people present their real identity. Other online groups encourage or even require people to assume an imaginary persona in video games in virtual world. Some video games in virtual worlds fall somewhere in between reality and fantasy, where people pretend to be someone very different than in reality or they can alter some features, such as the name, the occupation, or the physical appearance, while retaining the other true characteristics. Thus, dreams and fantasies of people disclose hidden aspects about what they need or want to be.

1.4.Level of conscious awareness and control

How people decide to present in cyberspace is not always a purely conscious choice. A person my select a username or avatar as he/she wishes, without completely understanding the symbolic and profound meaning of this choice. Also, this person may join an online group, because it seems interesting while failing to realize the motives concealed in that decision. Anonymity, fantasy, and numerous variety of online environments give ample opportunity for this expression of unconscious needs and emotions.

People vary greatly in the degree to which they are consciously aware and control their identity in cyberspace. For example, some people who play the role of imaginary characters report how the characters may take a life of their own.

People who surrendered their normal identity to the imaginary persona perhaps later understand the meaning of this transformation.

1.5.The Media chosen

People express their identity in the clothes they wear, in the body language, through the careers and hobbies they pursue. Similarly, in cyberspace, people choose a specific

communication channel to express themselves. In cyberspace there are a variety of communication channels that express different aspects of the identity. For example, people who rely on text communication prefer the semantics of language and perhaps also the linear, composed, rational, analytic dimensions, of self that surface via written discourse. Some people prefer synchronous communication, like chat groups, which reflect the spontaneous, free-form, witty and temporally present self. Others are drawn to the more thoughtful, reflective, and measured style of asynchronous communication, as in e-mail messages and blogs.

2. IDENTITY THEFT IN CYBERSPACE

European Commission recently said that identity theft was not criminalised yet across all the Member States of the European Union (Commission Of The European Communities. Communication From The Commission To The European Parliament. The Council and The Committee of the Regions, 2007). The European Commission said will commence consultations to assess if legislation is appropriate.

Not all the countries implemented provisions in the national systems of criminal law that criminalize all the acts related to identity theft.

The term *identity theft* describes criminal acts through which the perpetrator fraudulently obtains and uses another person's identity (Gercke, 2007, p. 4). These acts can be carried out by using information and communication technology. Internet-related identity theft cases are to a large extent based on highly sophisticated scams and show the difficulties that law enforcement agencies are faced with when investigating such offences (Clough, 2011, pp. 145-170).

It is important to make a difference between the term *identity*, approached from the philosophic and sociologic point of view, which is used to describe the totality of elements which form the identity of a person and the target of the identity theft. As for the offence of identity theft, we must highlight the fact that it is not necessary that the offender obtain all the data related to the victim's identity. Certain information data, such as passwords, account data and information necessary to access the information system, which does not represent elements of the legal identity related to a person, offers the offender the possibility to illegally access other personal computer data which is used to establish the victim's identity (Clarke, 2004, pp. 55-63).

Among the methods frequently used by offenders to obtain identity-related data we mention as follows: (Gercke, 2007, pg. 14-16)

- *Physical methods*

Physical methods refer to computer storage devices with identity-related data. According to a survey, it was highlighted the fact that were committed more computer-related offences with regard to the theft of confidential computer data and mobile hardware (Computer Security Institute, 2007, p. 15).

- *Search engines and file-sharing systems*

Search engines and file-sharing systems are used by offenders to identify and obtain identity-related data. Search engines enable the users to search millions of web pages within seconds, this technology not being used only for legitimate purposes. *Googlehacking* and *googledorks* are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to

computer security issues as well as personal information that can be used in identity theft scams. In the literature (Gercke, 2007, p. 15) it was highlighted that the file-sharing software can not only be used to search for music and video files stored on the computer of other users of the file-sharing network, but also for private information.

- *Insider attacks*

Insiders, who have access to stored identity-related information, can use their access to obtain that information.

- *Attacks from the outside*

Attack from the outside is carried out through the offence of illegal access to a computer system (hacking). Attacks from the outside involve the use of malicious software, like spyware[1] and keylogger[2].

- *Social engineering regarding the disclosure of identity-related information*

Offenders can use social engineering techniques to persuade the victim to disclose personal information. In recent years, offenders developed effective scams to obtain secret information (e.g. bank account information and credit card data), by manipulating users through social engineering techniques (Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, 2001, p. 1). Phishing is an example of social engineering regarding the disclosure of identity-related information (Jakobsson, 2007, p. 10). Phishing is a practice to send false e-mails or spam, written to appear as if they were sent by banks or other respectable organizations, with the intention to disclose important information, such as usernames, passwords, account IDs, PIN codes of credit cards. Typically, phishing attacks will lead the recipient to a Web page designed to simulate the own visual identity of a target organization, and to collect personal information about the user, the victim not being aware of the attack.

There is no standard definition regarding identity theft. The only element which is found in the definitions regarding identity theft is that it is carried out in several phases: (Gercke, 2007, p. 14)

1. Act of obtaining identity-related information.
2. Act of possessing or transferring identity-related information.
3. Act of using identity-related information for criminal purposes.

Based on this observation there are, in general, two systematic approaches with a view to criminalising identity theft:

- Creation of a single provision which criminalizes the offence to obtain, possess and use identity-related information for criminal purposes;
- Individual criminalization of offences related to obtaining identity-related information, such unlawful access, producing and diffusion of malicious software, computer falsification, data espionage, affecting of integrity of data as well as of offences related to the possession and use of such information, such as computer fraud.

The most known example of such approach regarding a single provision refers to the stipulations of the Federal Criminal Code of the United States of America, which is Title

[1] Spyware is the general term used to describe a software which violates the personal security of the user. By its nature, spyware is capable of collecting and transferring personal information, such as e-mail addresses, usernames, passwords and credit cards numbers.

[2] Keylogger is a small hardware device or a program which registers each key which a user presses and sends the information to the person who installed the device or the program.

18, Part I, Chapter 47, Section 1028(a)(7)[3]; Title 18, Part I, Chapter 47, Section 1028A(a)(1)[4] (Aggravated identity theft).

Criminalization of identity theft in the Federal Criminal Code of the United States of America, specifically in Section 1028 (Fraud and related activity in connection with identification documents, authentication features, and information) and Section 1028A (Aggravated identity theft) is not limited to one of the three phases, this criminalization covering all the three phases through which identity theft is carried out. Sections 1028 and 1028A of the Federal Criminal Code of the United States of America create distinct offences that, apart the offences they are related to[5], criminalize the transfer, the possession and the use of the means of identification of a person in relation to the commitment of an illegal act.

The Council of Europe Convention on cybercrime uses the approach regarding the individual criminalization of acts related to obtaining identity-related information. The Council of Europe Convention on Cybercrime does not contain a general provision to cover any approach regarding obtaining, possessing and using identity-related information for criminal purposes. Moreover, I consider that this legal instrument does not create a distinct offence which criminalizes illegal obtaining, possessing and using identity-related information in case of committing some computer offences, but criminalizes certain acts in relation to the identity theft offence.

The Council of Europe Convention on Cybercrime and Directive 2013/40/UE[6] of the European Parliament and the Council of 12 August 2013 on attacks against information systems criminalize a number of acts which are related to phase 1 which refer to the act of obtaining information related to identity, as well as phase 3 which refers to the act of using identity-related information for criminal purposes.

With regard to phase 1, the *Act of obtaining identity-related information*, the Convention has a number of provisions criminalizing the acts of identity theft through Internet: (Seger, Identity theft and the Convention on Cybercrime, 2007, p. 3)

- Illegal access (ART.2 of the Convention);
- Illegal interception (ART.3 of the Convention);
- Data interference (ART.4 of the Convention);
- System interference (ART.5 of the Convention);
- Misuse of devices (ART.6 of the Convention);
- Computer-related forgery (ART.7 of the Convention).

With regard to phase 1, we highlight the existence of other illegal acts that are related to this phase and are not covered by it. Such example is that offence which is often related to phase 1 of the identity theft and which is not covered by the Convention, this being *data espionage*.

---

[3] Cornell University Law School. U.S. Code. Retrieved 19 December 2014 from http://www. law. cornell.edu/uscode/text/18/1028.

[4] Cornell University Law School. U.S. Code. Retrieved 19 December 2014 from http://www.law .cornell.edu/uscode/text/18/1028A.

[5] „Any illegal activity which constitutes a violation of the federal right" according to the provisions of Section 1028(a)(7); „Any violation listed in subsection c" within Section 1028A.

[6] Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Retrieved 21 February 2015 from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN.

The provisions of article 7 of the Convention covers the acts of identity theft through Internet, as the enforcement bodies investigate also the phishing cases based on e-mail.

As for phase 2, the *Act of possessing or transferring the identity-related information* is not comprised in the provisions of the Convention (Seger, Identity theft and the Convention on Cybercrime, 2007, p. 3).

Phase 3, called the *Act of using identity-related information for criminal purposes* is mentioned in the Convention through article 8 which refers to computer-related fraud (Seger, Identity theft and the Convention on Cybercrime, 2007, p. 3). An example of computer-related fraud which uses identity theft is the fraud through credit cards.

The identity theft offence is stipulated also by the legislation from the United Kingdom, specifically in Identity Cards Act 2006[7]. This act contains, in addition to offences related to identity cards, the provisions regarding to punishment of abuses on identity cards (Levi & Burrows, 2008, pp. 293-318). All the acts in relation to the offence of identity theft are stipulated by the Identity Cards Act 2006 from article 25 to article 30. This legislative act through the criminalization related to identity theft comprises in articles 25-30 covers all the three phases through which identity theft is carried out through Internet.

The offence of identity theft is also stipulated by the legislation in Australia, in the Criminal Code Act 1995[8]. This legislative act contains in Part 9.5., called *Identity crime*, the provisions related to identity theft, which are comprised by articles 370-376. Criminal Code Act 1995 covers the three phases through which is carried out the identity theft committed through Internet.

At the level of the European Union, an important role in criminalizing identity theft is Directive 2013/40/UE of the European Parliament and the Council of 12 August 2013 on attacks against information systems, through which the Member States of the European Union must elaborate effective measures against identity theft and other identity-related offences. At article 9 (5) of the Directive, Member States shall take the necessary measures to ensure that illegal system interference (art.4) and illegal data interference (art.5), when committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law. With regard to phase 1, the *Act of obtaining identity-related information*, Directive 2013/40/UE on attacks against information systems contains a number of provisions which criminalize the acts of identity theft through Internet:

- Illegal access to information systems (Art.3 of the Directive);
- Illegal system interference (Art.4 of the Directive);
- Illegal data interference (Art.5 of the Directive);
- Illegal interception (Art.6 of the Directive).

Phase 2, the *Act of possessing or transferring identity-related information* is not comprised in the provisions of the Directive. Phase 3, called the *Act of using identity-related information for criminal purposes* is mentioned in the Directive through article 7 which refers to tools used for committing offences. Pursuant to the provisions of article 7,

[7] Identity Cards Act 2006. Retrieved 19 December 2014 from http://www. legislation.gov .uk/ukpga/2006/15/contents.

[8] Criminal Code Act 1995. Retrieved 19 December 2014 from http://www.austlii.edu.au/au/legis/cth/consol_act/ cca1995115.txt.

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, of the following tools: a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6, a computer password, access code, or similar data by which an information system is capable of being accessed.

The offence of identity theft is not regulated expressly in the Romanian criminal law legislation. However, I consider that the offence of identity theft could be criminalised by the following existent provisions in the Romanian Criminal Code: Article 360 which refers to illegal access to an information system; Article 361 which refers to illegal interception of a transmission of computer data; Article 362 which refers to alteration of integrity of computer data; Article 363 which refers to hindering of the functioning of information systems; Article 364 which refers to unauthorised transfer of computer data; Article 365 which refers to illegal operations with computer devices or programmes; Article 249 which refers to computer-related fraud; Article 325 which refers to computer-related forgery. All these illegal acts criminalised by the Romanian Criminal Code covers all the three phases through which identity theft is carried out through Internet.

3. CONCLUSIONS

Comparing the approach of the Federal Criminal Code of the United States of America regarding identity-theft and the Council of Europe Convention on Cybercrime, as being the most important legal instrument at European and international level in the area of fighting against criminality in cyberspace, I noticed the fact that there is a significant difference. This difference is related to the fact that the provisions of the Council of Europe Convention on Cybercrime protect various legal aspects such as the integrity of a computer system but not the integrity of identity-related information.

In general, identity theft is used for the preparation of further criminal acts, such as computer fraud. Even if identity theft is not criminalised as a separate act, in most countries law enforcement agencies will be able to investigate the subsequent offences. However, the main reason that nevertheless some countries have decided to criminalise identity theft as a separate offence is the fact that it is often easier to prove the crime of identity theft than the subsequent crimes. Perpetrators can use the obtained identities to hide their own identity. Thus, I appreciate the fact that legislators of the Convention should supplement its provisions, in the sense to establish a legislative framework based on a specific provision that is focusing on identity-related information as the subject of legal protection, therefore covering the identity theft committed through the Internet.

REFERENCES

Clarke, R. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research, Volume 10, Issue 1* , 55-63.

Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. *Criminal Law Forum, Volume 22, Issue 1-2* , 145-170.

Commission Of The European Communities. Communication From The Commission To The European Parliament. The Council and The Committee of the Regions. (2007). *Towards a general policy on the fight against cyber crime.* Strasbourg: Council of Europe.

Computer Security Institute. (2007). *Computer Crime and Security Survey* . Orlando: Computer Security Institute.

Gercke, M. (2007). *Internet-Related Identity Theft.* Strasbourg: Council of Europe. Economic Crime Division. Directorate General of Human Rights and Legal Affairs.

Granger, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics.* Mountain View, California: Security Focus.

Jakobsson, M. (2007). *The Human Factor in Phishing.* Bloomington, Indiana: School of Informatics, Indiana University at Bloomington.

Levi, M., & Burrows, J. (2008). Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology* , 293-318.

Seger, A. (2007). Identity theft and the Convention on Cybercrime. *UN ISPAC Conference on the Evolving Challenge of Identity-related crime* (p. 10). Courmayeur, Italy: Council of Europe.

Suler, J. (2002). Identity Management in Cyberspace. *Journal of Applied Psychoanalytic Studies* (4), 455-460.