THEMIS

IDENTITY THEFT: A GROWING THREAT

Challenges, Posed by Identity Theft as a Step Towards Terrorism

Themis competition
Semi - final A
12-14 April 2016

TEAM BULGARIA:

Emilia Ganeva
Candidate junior prosecutor

Yoana Vangelova
Candidate junior judge

Valentina Penchovska
Candidate junior prosecutor

Aneliya Shtereva
Judge

IDENTITY THEFT: A GROWING THREAT

TABLE OF CONTENTS

INTRODUCTION

What exactly is the object of ID theft and why is this act so attractive to terrorism?

The specific of this kind of "theft", is related to its object, therefore the first question that should be answered is how can the "identity" be defined and identified?

The identity is necessarily linked to the notion of person. We can derive the meaning of this second term from the ancient Roman law, where this concept was expressed by the term "*persona*" coming from the Latin words "*per*" and "*sono*" with literal meaning "sound through", i.e. someone whose voice sounds through the mask, first in the theatre, then in the court and community. The idea of this concept was that between the individual inside and the individual who can be seen from the outside exists a difference. *Persona*, in fact, expressed the external side of the individual, providing him the opportunity to participate in all the aspects of society, or in a particular one (for example, as a plaintiff or a defendant in the court). Only this part of an individual's personality was visible for the other members of the community.

In the modern times, we can conclude that the object of "identity theft" is exactly this part – someone's social mask. This act of obtaining someone else's identity today is easier than it was years ago. It is because of the greater complexity of the concept and because of the greater number of material and immaterial information carriers of these personal data, which are the contemporary equivalent of the ancient mask. Nowadays "identity" as a concept, includes a lot of personal information like, for example, *"...gender, first and last name, date and place of birth, parents' first and last name and in some countries, individuals' assigned social security number…. Individuals also can be identified with a variety of other attributes including a computer username and password, a web page, a blog, an Internet Protocol (IP) address that identifies computers on the Internet, an e-mail address, a bank account and PIN number,… contained in official documents such as passports, identity card, birth and death certificates, social security numbers or driving licences"[1],* etc. This shows that the data that could be a particular object of ID theft are extracted from off-line and on-line sources.[2]

1 Scoping paper on Online Identity theft, Ministerial Background report DSTI/CP (2007)3/FINAL, OECD Ministerial meeting, Seoul, Korea, 2008, p.15, (15 footnote)

2 More details about methods for on-line and off-line obtaining of personal data see in Final report, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, CSES, 2012, p. 34-47

The more global the world becomes, the harder it is to protect these data, which means that the hazards in relation to the misuse of personal information for achieving illegal aims is greater.

All these data give society the opportunity to identify an individual, i.e. to identify who stays under the mask. On the basis of this kind of information the community makes the presumption that the person who claims to be someone is exactly this someone. But we must not forget that this presumption is rebuttable. All this information is frequently used by others with intention to participate in various illegal activities such as fraud, obtaining credit, money, goods, services, employment benefits[3] and terrorism, under the stolen identity. All these crimes united under the common term identity-related crimes *"acquired a prominent place in the crime prevention and criminal justice agenda of the United Nations"*. [4]

In the current study we emphasize on terrorist attacks as crimes where the "identity theft" is both a target and a tool. Such kind of criminal activities are facilitated nowadays by the huge immigrant stream flooding Europe.

It has to be highlighted that preventive legal measures against this kind of theft must be taken because *"ID thieves may sometimes not use the victims' identity themselves to commit fraud. Instead, they will sell it to other parties who will themselves commit fraud, or generate new illegal forms of personal identity (such as a birth certificate, driver's license, or a passport)"*[5]. Because of that, the act of taking the identity on its own ground causes a high level of danger to the community.

1. DEFINITIONS[6]

Nor on EU neither on international level exists common legal framework, respectively common concept of what ID theft is. There are many and diverse definitions, which can be found in legal sources and surveys of different states and organisations.

3 Scoping paper on Online Identity theft, footnote 1, p. 15

4 See the Handbook on Identity-related Crime, United Nations, April 2011, p. 38; Bangkok Declaration, Synergies and Reponses: Strategic Alliance in Crime Prevention and Criminal Justice", 2005 endorsed by General Assembly resolution 60/177 of 16 December 2005

5 Scoping paper on Online Identity theft, footnote 1, p. 15

6 About the different definitions see Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report TR-982-EC, RAND Europe, 2011, Comparative overview of definitions, table 4, p. 10-12; All the definitions in the current study for which there isn't a reference are quoted by the mentioned table 4 in this Comparative Study.

The existing definitions for the purpose of our study are conditionally separated into several categories:

The first category includes definitions which do not make a clear difference between the act of ID theft and the act of ID fraud*:*

- *"**Identity theft** […] occurs when one person […] obtains data or documents belonging to another—the victim—and then passes himself off as the victim".* [7]

- *"**Identity 'theft**' is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent."* [8]

- *"Someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existent person".* [9]

- According to UK Home Office Identity Fraud Steering Committee *"**Identity theft** is also known as impersonation fraud. It is the misappropriation of the identity (e.g., name, date of birth, current or previous addresses) of another person without their knowledge or consent."*

- Similar approach of defining ID theft can be seen in The United States Federal Trade Commission's definition: *"Credit card fraud (25 %) was the most common form of reported identity theft".* [10]

From the analysis of these definitions, it can be concluded that the crime contains the following substantive characteristics of corpus delicti: the identity information which is the object of the crime and the act of the crime which is a complex activity consisting of obtaining and subsequent use of identity information. It can be seen that in some definitions *"identity theft"* and *"identity*

7 N. Mitchison, M. Wilikens, L. Breitenbach, R. Urry, S. Portesi, Identity Theft A Discussion Paper, European Communities, 2004, p. 5

8 B.-J. Koops, R. Leenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 30 (2006) 9, p. 556

9 J.H.A.M. Grijpink reference to 'Identiteitsfraude als uitdagiing voor de rechtstaat (Identity Fraud as a Challenge to the Rule of Law), Privacy & Informatie, (2003) (followed also in FIDIS (2006), we extract the definition from the Comparative Study, footnote 8, p. 8; Similar approach is adopted by J.H.A.M. Grijpink in Biometrics security Trend report on biometrics: some new insights, experiences and developments, Ministry of Justice/Utrecht University, 2008, p. 1

10 Consumer fraud and Identity theft Complaint data, 2006, Federal Trade Commission 2007, p. 3; Similar approach in defining ID theft we see in Consumer Sentinel Network data book, Federal Trade Commission , 2014, p. 3

fraud" are used as substituents of one another. In other cases, the definitions are constructed in different way since *"identity theft as the initial activity… is followed up subsequently by identity fraud"*[11]. And also sometimes identity theft can be understood *"as a subset of identity fraud"*.[12] The concept of ID theft, derived from these examples is a mix of two concepts that are usually separated in most legislations. These are the concepts that are staying under the terms "theft" and "fraud" [13], which are frequently used together to define this kind of illegal activity. We see that in this approach of constructing the definitions "theft" implicitly includes "fraud" or other crimes, which represent a subsequent illegal activity, following the simple act of obtaining someone's identity. The obvious reason is that in these cases the accent is on the illegal use of impersonation, but this act is an inseparable whole with the act of acquisition of ID.

The second category includes definitions, which make a difference between the act of obtaining of ID and the act of its use:

- *"Identity "theft" may be used to describe the theft or assumption of a pre-existing identity (or significant part of it) with or without consent, and regardless of whether the person is dead or alive."*[14]

- Legal provisions defining "identity theft" and identity-related crimes in the US legal regulation. According to the provision 18 U.S.C. § 1028(a) (7) identity theft is: *"Knowingly **transfers, possesses, or uses**, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."*

In this text the illegal acts of transferring, possessing and using this information are separate and every one of them constitutes a meaningful whole with the special intent for illegal activity, expressed by the words: to commit, or to aid or abet, or in connection with.

11 Comparative Study, footnote 8, p.6

12 Supra footnote, p 6

13 See also: Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, p. 9: the definition which use only the term "fraud" to define similar phenomenon, otherwise expressed by the term "theft", for example UK Cabinet Office: "**ID fraud** arises when someone **takes over** a totally fictitious name or **adopts** the name of another person with or without their consent"

14 The Handbook on Identity-related Crime, footnote 4, reference to Paget, Identity Theft, McAfee White Paper, 2007, p. 5

It has to be emphasized that in provision 18 U.S.C. § 1028A (1)(2) there is an **aggravated identity theft** in cases of felony violation, and especially in case of terrorism offense, as we can see:

"(a) Offenses.— (1)In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) Terrorism offense. Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B)[15], knowingly ***transfers, possesses, or uses****, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years."*

- In 2008 OECD's Committee for Information, Computer, and Communications Policy, offers the following definition: "***ID theft*** *occurs when a party* ***acquires, transfers, possesses, or uses*** *personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes*."[16]

This definition deserves attention because it covers both individuals and legal entities, and among the criminal acts except "transfers", "possesses", "uses", which we found out in the provision 18 U.S.C. § 1028(a)(7), 1028A(1)(2), there is also the term "acquires". By this term, we see clear demarcation between the act of obtaining of identity as a separate illegal activity and the acts of its use. This approach provides an opportunity for preventive regulation of the subsequent crimes, which the acquisition of identity theft facilitates.

Such an approach in constructing the definitions is well explained by Collins[17], who indicates that: "*Identity theft, however, is to be distinguished from identity crimes – those offences committed using the stolen personal or business identifying information – or 'identities.' Thus, the con-*

15 18 U.S. Code § 2332b - Acts of terrorism transcending national boundaries, (g)Definitions.—As used in this section, (5) the term "Federal crime of terrorism" means an offense that, (B) is a violation of— relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons),…etc.

16 Scoping paper on Online Identity theft, footnote 1, p. 3

17 Comparative Study, footnote 8, p. 6, reference to Collins (2005), cited in Sproule & Archer (2007)

ceptual relationship between identity theft and identity crime is that the former facilitates the later. In short, stolen identities are used to commit many other crimes which is why identity theft also can be viewed as an all-encompassing or overarching megacrime."

The third category of definitions could be called "identity-related crimes" which have a wider scope than those of the other two categories.

On the first place, it covers sub-categories "identity theft" and "identity fraud", as we see in the Study on Fraud and the Criminal Misuse and Falsification of Identity in 2007 of The United Nations Intergovernmental Expert Group.

Furthermore, there are definitions like the following: *"Identity-related crime concerns all punishable activities that have identity as a target or a principal tool"18*. This definition is too general and covers a broader scope of crimes, which are committed due to or in relation with identity theft or identity fraud.

It can be seen that, under the term "identity related crimes" two types of wrongdoings could be understood: on the one hand, these could be crimes that are subsequent activity which follows the act of the identity acquisition, because the latter is only the preliminary activity. On the other hand, this term could cover all crimes, including identity theft.

We think that the specification of identity-related crimes has to be done in the particular context of the unlawful activity.

In the countries, where a separate legal regulation of "identity theft" and a legal definition of the phenomenon do not exist, a concept similar to the above mentioned third category is indirectly achieved. This means that in these states there is a relatively broad scope of crimes, which have in common the misuse of impersonation. The problem in these countries is most frequently covered by other provisions regulating crimes as fraud, forgery or cybercrime, etc. For instance *"no legislation has been introduced in Bulgaria that focuses explicitly on identity theft as a specific crime, or that defines such a crime"19*. Although, The Bulgarian Criminal Code contains legal norms which provide punishments for crimes that cover most of the identity related crimes.

18 Koops, Leenes, Identity Theft, footnote 10, p. 556.; Also see the Handbook on Identity-related Crime, footnote 4, p 25-26

19 Comparative Study, footnote 6, p. 47

To raise public awareness useful information about hypotheses of "ID theft" are published on the web side of Bulgarian Ministry of Interior: http://www.cybercrime.bg/bg/internet/f04ff8/ [20]. But in Bulgarian legislation there is no specific regulation that encompasses the preliminary criminal activity of illegal obtaining of identity preceding the criminal use of it. The lack of explicit provisions against theft of such kind in Bulgaria and in many other countries and especially the lack of common legal framework of the problem on European and international level have their negative effect in the context of effective prevention of many related crimes, including terrorism.

2. ATTEMPTS FOR LEGAL REGULATION OF IDENTITY THEFT AND IDENTITY-RELATED CRIMES

When we speak about the legal regulation of identity theft, we should know that there are no international legal acts, declarations, conventions or other obliging documents, dedicated specifically to this theme. Currently, legal frameworks, related to the criminalisation of identity theft only exist on a national level. There is no specific identity theft legislation, created by international organisations, dealing with criminal law topics. Most of the countries do not have specific criminal law regulation on identity theft. Only several countries make an exception – for example, Australia, Canada, Estonia, France, Portugal, Slovenia and The United States. The absence of specific legislation on identity theft does, however, not mean that it is not criminalised. National legislation in almost every State criminalises the activities, related to identity theft or including it. There are similar rules in the field of fraud, forgery and data protection.

2.1. United Nations

In the **Bangkok Declaration** the UN underlines *"the crucial importance of tackling document and identity fraud in order to curb organized crime and terrorism"* [21]. With this declaration, Member States are appealed *"to improve international cooperation, including through technical assistance, to combat document and identity fraud, in particular the fraudulent use of travel documents, through improved security measures, and encourage the adoption of appropriate national legislation."*[22]

20 Last visited on 20.03.2016

21 Bangkok Declaration, Synergies and Reponses: Strategic Alliance in Crime Prevention and Criminal Justice, 2005, Paragraph 27, available at: http://www.un.org/events/11thcongress/declaration.htm (last visited on 20.03.2016).

22 Supra footnote.

The Economic and Social Council of The UN (ECOSOC) established **Resolution 2004/26 International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Fraud, the Criminal Misuse and Falsification of Identity and Related Crimes**. With this resolution the ECOSOC encourages Member States *"To take into account the need to prevent and combat fraud and the criminal misuse and falsification of identity in the development" 23*. It *"also encourages Member States to cooperate with one another in efforts to prevent and combat fraud and the criminal misuse and falsification of identity, including through the United Nations Convention against Transnational Organized Crime and other appropriate international instruments, and to consider the review of domestic laws on fraud and the criminal misuse and falsification of identity, where necessary and appropriate, to facilitate such cooperation".24*

On the basis of this resolution, The United Nations Office on Drugs and Crime launched a study on fraud and falsification of identity. *25*

Pursuant to UN Commission on Crime Prevention and Criminal Justice's **2007 Resolution on International Co-operation in the Prevention, Investigation, Prosecution and Punishment of Economic Fraud and Identity-related Crime**, UNODC established a consultative platform. The idea was to gather representatives from governments, international organisations and NGOs to work together on the problems of identity-related crimes and to share good practices.

The Report of the Secretary-General of the UN on recommendations for a global counter-terrorism strategy (2006) *26* focuses on strengthening the capacity of the United Nations to combat terrorism. One of the discussed problems is referring to the need „*to address the loopholes in transport security and to assists States in developing tools to tackle identity theft and fraudulent travel documents" 27* The importance of denying terrorist access to travel is highlighted. There is also a recommendation, connected to identity theft. It underlines the necessity to *„tackle the criminal trade in illegal documents that acts as an enabler to the terrorists' goals."28* As an effective tool in the fight

23 Resolution 2004/26 - International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, Paragraph 2 (b)

24 Resolution 2004/26 , Paragraph 3

25 See the Handbook on Identity-related Crime, footnote 4, p. 39

26 Uniting against terrorism: Recommendations for a global counter-terrorism strategy, Report of the Secretary-General of the UN, April 2006

27 Supra footnote, Paragraph 62

28 Supra footnote, Paragraph 63

against terrorism is pointed out Interpol's database on stolen and lost travel documents, which can help stop terrorists' attempts to cross the border. Promoting the rule of law, respect for human rights, promoting quality education and religious tolerance, ensuring transport security, improving information sharing are among the other measures, included in the report.

2.2. The International organisation helping governments tackle the economic, social and governance challenges of a globalised economy (OECD)

The OECD Council approved a series of guidelines, related to the protection of electronic commerce – for example, the **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980),** incorporating the principles of protection of privacy and personal data. The **Security Guidelines of Information Systems and Networks (2002)** aim to create a unified approach for overcoming the global security hazards, related to the transfer of data. The **Cross-border Fraud Guidelines (2003),** concern the determination of a *"common framework to combat online and offline cross-border fraud"* [29] through cooperation.

These guidelines are not legal documents, but can be used to develop measures or strategies for prevention of identity theft.

2.3. European Union

The European Union is also engaged in the matters of identity-related crimes.

In this regard, **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data** can be mentioned**.** Its goal is to provide privacy of personal data, without restricting its free flow (Art. 1).

The EU Council **Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment** also concerns some aspects of ID-related crimes. It prescribes the criminalisation of specific types of fraud.

These instruments are indirectly connected with identity-related crimes, but they do not cover identity theft as a separate crime.

Directive 2002/58/EC on privacy and electronic communications concerns the processing of personal data and the protection of privacy in the electronic communications sector.

29 Scoping paper on Online Identity theft, footnote 1, p. 45

"This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community"30.

In July 2007, The Commission adopted a **Comparative study on legislative and non-legislative measures to combat identity theft and identity-related crimes** that includes definitions of identity theft, used in the EU Member States. The Final report of the comparative study concentrates on different measures to combat identity theft and identity-related crimes. *"This report represents a multi-stage legislative and policy diagnostic intended to assess the validity and effectiveness of current EU Member States' legal and non-legal responses to the particular public policy challenge of the emergence of identity theft." 31* Important issues relating to the emergence of identity theft and related crimes are highlighted. The role of technology and its impact on the mechanism of committing identity-related crimes is also discussed.

The EU institutions are supported by a number of agencies and bodies in the combat against cybercrime. Among them Europol and The EU Contact Network of Spam Enforcement Authorities should be mentioned. The latter is aimed at exchanging information and best practices in the domain of anti-spam legislation. In 2006 The European Network and Information Security Agency made a research about security measures, regarding internet services and anti-spam activities.

The Council **Framework decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters** is another EU instrument. Its purpose according to Art. 1 (1) is *"to ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters."*

30 Directive 2002/58/ec of The European Parliament and of The Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Art. 1

31 Comparative Study, footnote 6, Preface

The Council of the European Union launched a number of strategies. One of them is **The European Union counter-terrorism strategy (2005)** *32.* It covers four areas – prevention, protection, pursuit and response. It concentrates on finding a way to combat terrorism globally while respecting human rights. According to the strategy Member States should: improve national capabilities, work together to share information, establish a collective policy and cooperate with The United Nations and other organisations.

Another strategy was launched in **2015**. It takes into account "*the necessity for the European Union to contribute to the protection of European citizens with regard to on-going increase of threats in particular posed by terrorism and serious and organised crime"33*. In the field of European Union internal security are underlined key issues regarding the prevention of terrorism, radicalisation to terrorism and recruitment as well as financing terrorism, fighting cybercrime and enhancing cyber security. In relation to these problems arises the need to establish a common legal framework and to actively cooperate with third countries.

2.4. Council of Europe

We consider the Convention on Cybercrime (2001) to be the most significant COE act, regarding the current topic. It prescribes the criminalisation on a national level of the following activities: illegal access (Art. 2) and illegal interception to computer data (Art. 3), data interference (Art. 4), system interference (Art. 5), misuse of devices (Art. 6), computer related forgery (Art. 7), computer related fraud (Art. 8) *34*.

2.5. Interpol

As an organisation facilitating international police cooperation, Interpol launched a best practice guide called ***„The Information Technology Crime Investigation Manual".*** Furthermore, Interpol created the G8 24/7 High Tech Crime Network, which enables experts from all over the world to communicate easier and faster. *35*

2.6. Asia-Pacific Economic Cooperation

In 2002, APEC launched ***The Cyber Security Strategy***. This strategy includes recommendations for criminalisation of cybercrime. In 2005, APEC launched ***The Strategy to Ensure a Trusted,***

32 Council of the European Union, 30 November 2005, The European Union Counter-Terrorism Strategy

33 Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020

34 The Convention is discussed in the Scoping Paper on Online Identity Theft, footnote 1, p. 50

35 Supra footnote, p. 47-48

Secure and Sustainable Online Environment concerning addressing the threat of misuse and criminal use of online environment.

3. CASES

18th July 2012, Burgas, Bulgaria. A bus, transporting Israeli tourists exploded outside Burgas airport, killing seven – five of the tourists, the Bulgarian driver and the alleged bomber. Investigators managed to recover two US driving licenses, probably used by the perpetrators of the terrorist act. Later Europol announced that forensic and technical examination proved that the identity documents were both counterfeits from the same source, located in Lebanon *36*.

13th November 2015, Paris, France. A series of seven coordinated terror attacks resulted in 130 victims and shattered Europe. A few days later the Belgian authorities released information that they were searching for two suspects, linked to the Paris attacks, travelling with fake Belgian identity cards*37*.

Both cases come to show that identity-related crime and terrorist attacks can be closely connected. As a matter of fact, the collection of personal data for the needs of forging identity documents can be part of the preparation of a terrorist act. This could, at the same time, affect the personal rights of the victim of the identity theft *38* and impede the prevention of the crime or the prosecution of its true perpetrator. Therefore, the problems, posed by identity theft, should be addressed as part of the fight against terrorism, including with the tools of international cooperation.

4. INTERNATIONAL COOPERATION

International cooperation is always crucial when it comes to combating transnational crime. Both terrorism and identity-related crime (especially online identity theft) usually involve a multitude

36 See https://www.europol.europa.eu/content/europol-supports-investigation-terrorist-attack-burgas-airport-bulgaria (last visited on 20.03.2016)

37 See http://www.telegraph.co.uk/news/worldnews/europe/belgium/12034240/Belgian-police-hunt-two-armed-and-dangerous-new-terror-suspects-over-Paris-attacks.html (last visited on 20.03.2016)

38 ECHR, Art. 8 Right to respect for private and family life

of participators and affect a large range of victims, often situated in various countries. Therefore, the investigation and prosecution of such acts generally require the joint efforts of several States.

Traditional instruments of international cooperation such as extradition, the European arrest warrant, mutual legal assistance and joint investigation teams are all applicable in the fight against identity theft as part of the preparation of terrorist acts. However, the criminal activities, subject of the present study, pose some specific problems regarding the use of conventional mechanisms due to the lack of a common legal regulation of identity-related crimes on European and international level.

4.1. Extradition

Extradition is one of the oldest instruments of international cooperation. It allows one State (requested State) to surrender to another (requesting State) a person against whom the competent authorities of the requesting State are proceeding for an offence or who is wanted by the said authorities for the carrying out of a sentence or detention order (Art. 1 of the European Convention on Extradition).

Subject of the following paragraphs will be some of the requirements for extradition in light of the problems, posed by identity theft as part of the preparation of terrorist acts. *39*

According to most conventions extradition has a limited scope and can only be applied for *serious offences 40*. Identity theft as a step towards committing a terrorist act is by all means a crime of great gravity and can meet this requirement.

The *double criminality* principle is adopted by all extradition treaties, but there are different approaches to its definition. Some treaties contain a list of crimes, for which this instrument is applicable. Others allow its use, whenever certain conduct is criminalised in both requesting and requested State. Given that identity theft is amongst the so-called emerging crimes, this requirement

39 For more details see the Handbook on Identity-related Crime, footnote 4, p. 246-252.

40 For example, Art. 2 (1) of the European Convention on Extradition, Paris 1957 states the following: "Extradition shall be granted in respect of offences punishable under the laws of the requesting Party and of the requested Party by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty. Where a conviction and prison sentence have occurred or a detention order has been made in the territory of the requesting Party, the punishment awarded must have been for a period of at least four months."

raises specific questions. For instance, it is possible that identity theft is not criminalised in the requested State, which is a mandatory ground for refusal of extradition. However, if identity theft is a part of the preparation of a terrorist act, the double criminality requirement will in any case be met, as terrorism and the preparation of terrorist acts are criminalised in all modern legal systems.

Of course the principle of *non bis in idem* [41], as well as the *speciality rule* [42] must also be observed.

Another traditional principle is the one of *"non-extradition of nationals"* [43]. However, it is not unconditional and some States permit extradition in such cases. For example, according to Art. 25 (4) of the Constitution of the Republic of Bulgaria *"No Bulgarian citizen may be surrendered to another State or to an international tribunal for the purposes of criminal prosecution, unless the opposite is provided for by international treaty that has been ratified, published and entered into force for the Republic of Bulgaria."* The European Convention on Extradition, for instance, is such a treaty.

It must be noted that continental law States and common law States have different practices, regarding extradition procedure. According to continental law the judicial authorities of the requested State should not examine the evidence of guilt against the person sought, whereas common law demands the exact opposite approach. These differences can cause serious difficulties, which can delay and even impede the extradition procedure [44].

A number of conventions require that parties either extradite or prosecute a person, who has conducted or attempted to conduct a terrorist act or has participated as an accomplice in one [45]. The scope of such treaties can cover identity theft as part of the preparation of terrorist acts.

41 Art. 9 of the European Convention on Extradition, Paris 1957 "Extradition shall not be granted if final judgment has been passed by the competent authorities of the requested Party upon the person claimed in respect of the offence or offences for which extradition is requested. Extradition may be refused if the competent authorities of the requested Party have decided either not to institute or to terminate proceedings in respect of the same offence or offences."

42 Art. 14 (1) of the European Convention on Extradition, Paris 1957 "A person who has been extradited shall not be proceeded against, sentenced or detained with a view to the carrying out of a sentence or detention order for any offence committed prior to his surrender other than that for which he was extradited, nor shall he be for any other reason restricted in his personal freedom." There are exceptions to the speciality rule, namely in case the requested State consents or the extradited person, having had an opportunity to leave the territory of the State to which he was surrendered, does not do so within 45 days of his final discharge, or returns to that territory after leaving it.

43 See, for example, Art. 6 of the European Convention on Extradition, Paris 1957.

44 See the Handbook on Identity-related Crime, footnote 4, p. 251

4.2. European arrest warrant

The EAW is an instrument, used within the European Union, which differs from the extradition procedure in several aspects. First of all, expedition is amongst the basic principles in the mechanism of the EAW – the procedure is standardised and has strict time limits.

Another difference in comparison to extradition is that the double criminality rule does not apply for the offences, listed in Art. 2 (2) of the Framework Decision 2002/584/JHA, as long as they are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years. Some of these offences are of particular interest with reference to the subject of identity theft as part of the preparation of terrorist acts – namely, terrorism, computer related crime, facilitation of unauthorised entry and residence, forgery of administrative documents and trafficking therein.

In addition to this the Framework decision abolishes the "non-extradition of nationals" rule*46* and the political offence exception. Its Art. 27 (1) provides for a deviation from the rule of speciality*47*.

Furthermore, the issuing and execution procedure are entirely judicial. In some Member States executive authorities still play a certain role in the procedure, but it is limited to the administrative transmission and reception of the EAW. Others adopt a different approach – direct contact between judicial authorities. The latter makes cooperation more efficient, especially in the fight against identity theft, which requires taking prompt measures *48*.

45 See, for example, the Convention for the Suppression of Unlawful Seizure of Aircraft, The Hague 1970; the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Montreal 1971; the International Convention for the Suppression of Acts Nuclear Terrorism, New York 2005.

46 In relation to the surrender of nationals or residents of the executing Member State see Art. 5 (3) of the Framework Decision 2002/584/JHA.

47 Art. 27 (1) of the Framework Decision 2002/584/JHA "Each Member State may notify the General Secretariat of the Council that, in its relations with other Member States that have given the same notification, consent is presumed to have been given for the prosecution, sentencing or detention with a view to the carrying out of a custodial sentence or detention order for an offence committed prior to his or her surrender, other than that for which he or she was surrendered, unless in a particular case the executing judicial authority states otherwise in its decision on surrender."

48 See the Handbook on Identity-related Crime, footnote 4, p. 252-254

4.3. Mutual legal assistance

MLA can take different forms – e. g., a letter rogatory, examination of witnesses, interrogation of suspects, service of judicial documents, etc. The Convention on Cybercrime Budapest (2001), provides for several new forms of MLA, which can be efficiently used in identity theft cases. These new instruments include expedited preservation of stored computer data, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, mutual assistance regarding the real-time collection of traffic data and mutual assistance regarding the interception of content data.

When it comes to identity theft, it is of great importance that assistance requests are forwarded in a timely manner. In order to achieve that, expedited rather than conventional means of communication should be used *49*. Fax, e-mail, video and phone conference can help improve the efficiency of the cooperation.

Here, as well as in the extradition procedure and in the procedure, based on the EAW, usually stands the double criminality requirement, which would probably be met in most cases, related to the execution and preparation of terrorist acts.

International police cooperation is another efficient mechanism, which can and should be used in the fight against identity theft as part of the preparation of terrorist acts. Organisations such as Interpol and Europol can provide invaluable assistance in the process of investigation *50*.

4.4. Joint investigation teams *51*

The possibility of setting up joint investigation teams between Member States of the European Union is provided in the Convention on Mutual Assistance in Criminal Matters (2000) and the Framework Decision 2002/465/JHA. A JIT can also be set up by non-member States, as long as that is stipulated in a treaty, in a bilateral or multilateral agreement or in a national legislative act.

49 See the Handbook on Identity-related Crime, footnote 4, p. 256

50 For more details on the matters of MLA – the Handbook on Identity-related Crime, footnote 4, p. 254-258

51 For further details on this matter see the Joint Investigation Teams Manual, Brussels 2011

According to Art. 13 (1) of the 2000 MLA Convention and Art. 1 (1) of the above mentioned Framework decision a JIT is set up for a specific purpose and a limited period and its purpose is to carry out criminal investigations in one or more of the Member States, that set it up.

Eurojust and Europol play a significant role in the establishing and functioning of JITs. Both organisations can contribute in the process by giving legal advice and sharing good practices. They can, as well provide administrative, technical and financial support for Member States, setting up a JIT.

This instrument of mutual assistance can be particularly useful for the investigation of identity-related crime and terrorism. The cross-border nature of such criminal conduct inevitably affects the interests of multiple States, thus cooperation should be initiated at the very beginning of criminal procedures. Besides, JITs are a flexible mechanism, which facilitates the timely gathering of evidence and allows judicial authorities to react adequately to transnational crimes.

There are other unconventional forms of international cooperation, such as The London Action Plan, orientated against online threats like spam and the G8 24/7 High Tech Crime Network, which provides expert contact points, facilitating the exchange of information against cybercrimes*52*.

4.5. Jurisdiction

Determining jurisdiction in cases of identity theft as an element of the preparatory activity towards terrorism can be e a serious problem. When the identity theft itself is committed in one State, and the terrorist act – in another, both States could be entitled to prosecute the perpetrators on different grounds. This could lead to the so-called positive conflict of jurisdiction. The lack of an international legal framework results in a lack of regulation of this problem. That is why cooperation and coordination of action between the affected States is of primary significance. Only close contact and constant communication can help prevent conflicts of jurisdiction. *53*

52 Scoping Paper on Online Identity Theft, footnote 1, p. 48

53 About positive conflicts of jurisdiction with regard to MLA see the Handbook on Identity-related Crime, footnote 4, p. 257

CONCLUSION

The existing diversity of definitions of "identity theft" and "identity-related crimes" is one of the most serious obstacles to achieving a unified approach to regulate these phenomena. Thus, it is necessary to synchronize the conceptual apparatus on European and international level. Some steps have been made in that direction, but a legal definition has not yet been established.

We consider that in the process of creating a common definition the above mentioned approach, regarding the second category of definitions, should be taken into account. Thereby, the act of obtaining the ID will be criminalised separately from the subsequent criminal activity, related to illegal use of personal data. The advantage of this approach is the opportunity to prevent the occurrence of other identity-related crimes, including terrorism.

Should consensus be reached about a common definition, that would be a good ground for establishing a thorough international legal framework. This, in its turn, would facilitate the efforts of States to tackle the problems on a national level. On the other hand, it would have a positive effect on the opportunities for international cooperation.

The brief overview of traditional instruments of international cooperation shows that they can be applied in the process of investigation and prosecution of identity theft as a preparatory act towards committing terrorist attacks. However, they need to be adapted in order to answer the specific needs of the criminal procedures, initiated in relation to such crimes. As expedition is of primary importance in these cases, procedures should be simplified and informal contact between national institutions should be stimulated. Of course, international organisations such as Interpol, Europol and Eurojust play a key role in the process.

The lack of a common definition of identity theft and the different approaches of national legal systems, regarding its criminalisation at the present moment create further problems, especially with respect to the application of the double criminality principle. That is why efforts should be orientated to the faster unification of legal provisions in this sphere, as we already highlighted.

At the current moment the problems posed by identity theft are of great importance for Europe because of the immigrant stream. That is why these issues should be addressed by national authorities and international organisations with priority.

Terrorism, as a crime, is not interested in individualities – nor when it comes to perpetrators, neither when it comes to victims. The use of different masks, under which the terrorists cover their identity, is a frequently used method to conceal their activity. That is why efforts should be directed towards unveiling their true personality. Ultimately, the protection of an individual's social mask is protection of society.

BIBLIOGRAPHY:

- B.-J. Koops, R. Leenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 30 (2006) 9;
- J.H.A.M. Grijpink in Biometrics security Trend report on biometrics: some new insights, experiences and developments, Ministry of Justice/Utrecht University, 2008;
- N. Mitchison, M. Wilikens, L. Breitenbach, R. Urry, S. Portesi, Identity Theft A Discussion Paper, European Communities, 2004;
- Paget, Identity Theft, McAfee White Paper, 2007;
- Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report TR-982-EC, RAND Europe, 2011;
- Consumer fraud and Identity theft Complaint data, 2006, Federal Trade Commission 2007;
- Consumer Sentinel Network data book, Federal Trade Commission, 2014;
- Final report, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, CSES, 2012;
- Handbook on Identity-related Crime, United Nations, April 2011;
- Identity Fraud: A Study, United Kingdom Cabinet Office, 2002;
- Joint Investigation Teams Manual, Brussels, 2011;
- Scoping paper on Online Identity theft, Ministerial Background report DSTI/CP (2007)3/ FINAL, OECD Ministerial meeting, Seoul, Korea, 2008.