

From Nothing to having it All?: The Importation of Identity Theft by the EU*

Marta MUÑOZ DE MORALES ROMERO**¹

*Instituto de Derecho Penal Europeo e Internacional –
The Institute of European and International Criminal
Law*

I. Introduction

The first impression of the European jurist -at least the continental variety- when grappling with the problem of identity theft is one of absolute perplexity. Nothing will leave anybody with a feeling of indifference after reading pioneering articles in the field by well-known authors in American literature. Phrases and slogans such as "Don't be low hanging fruit, let it happen to someone else"; or, even, "How bad people get good credit"², etc., allow one to understand that the rationality of the politico-criminal discourse on this criminal matter raises considerable doubts. On this matter, an understanding of the meaning of theft and, in a wider sense, identity fraud has yet to be defined in the territory of the European Union (EU)³, except in the

case of the United Kingdom, and to a lesser extent in others, such as the Netherlands. In fact, the legal definition of identity theft as a crime in itself is hardly prevalent in the legal orders of the member States. However, this does not imply its imminent criminalisation over coming years. North American influence in criminal Law and even more so in Economic Criminal Law⁴, leads one to envisage a dramatic expansion of this branch of law, and, more specifically, a definitive legal definition of identity theft as a single criminal offence throughout the Union. The possibilities of including this new crime are certainly very extensive, as the tendency of particular countries "to copy" in a unilateral way, without consultation or debate, whatever is cooked up in the kitchen on the other side of the Atlantic, is backed up by the full force of international organizations and of course, the EU⁵, in order to harmonize the criminal laws of the member States. The basic purpose of this article is precisely to analyze the evolution of this criminal offence in a specific supranational organization, the European Union, from its most remote origins up to the present day

* This article has been compiled within the research project of the Junta de Comunidades de Castilla-La Mancha PC 108-0144-0952 with the title "El espacio europeo de seguridad y justicia y los nuevos desafíos para la protección penal de los derechos humanos en la globalización [The European area of freedom security and justice and the new challenges for the criminal protection of human rights in a globalized world]".

** This contribution has been made possible thank to the FPU grant from the Spanish Ministry of Education and Science through which it was financed over four years (1 March 2005/28 February 2009).

1 Critically, MONAHAN, T.: "Identity theft vulnerability: Neoliberal governance through crime construction", in *Theoretical Criminology*, 2009, p. 163.

2 Examples taken from and criticised in COLE, S.A./PONTELL, H.N.: "'Don't Be Low Hanging Fruit': Identity Theft as Moral Panic", in MONAHAN, T. (ed.): *Surveillance and security: technological politics and power in everyday life*, CRC Press, 2006, p. 129.

3 See *Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE):*

"Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview", European Commission, Joint Research Centre, July 2003, p. 19 and ff. (available at <http://www.jrc.es/home/publications/publication.cfm?pub=1118>).

4 NIETO MARTÍN, A.: "Americanización del Derecho penal económico", in *Revista Penal*, nº 19, 2007. Also in English "Americanisation or Europeanisation of corporate crime?" - which is adapted to the *grille* structure of DELMAS-MARTY in DELMAS-MARTY, M./SIEBER, U./PIETH, M.: *Les chemins de l'harmonisation pénale*, UMR de Droit comparé de Paris, vol. 15, 2008.

5 See DELMAS-MARTY, M./PIETH, M./SIEBER, U. (dir.): *Les chemins de l'harmonisation pénale/Harmonising Criminal Law*, Société de Législation Comparée, 2008 (first published in Spanish with a Prologue by Luis ARROYO ZAPATERO, Ed. Tirant lo Blanch, 2009). Specific fields are highlighted in this book in which the EU has been a relevant actor, as could not be otherwise in the case of the protection of the financial interests of the Community (See contribution by SOTIS), but also in the harmonization process relating to the fight against corruption (See contributions by MANACORDA and PIETH) and, in general, economic criminal law (See contribution by NIETO MARTÍN).

(II.), in order to go on to examine the legal instruments established in the constitutive Treaties that would make it feasible in the future to intervene in the field of criminal law, in order to harmonize this criminal offence throughout EU territory (III).

II. Evolution of the Politico-Criminal Discourse on Identity Theft in the European Union

1. First manifestations

Identity theft has only recently arrived on the scene and on the desks of community institutions. This phenomenon appeared not to warrant political concern in the EU until the beginning of 2000. The increase in the use of new technologies, on the one hand, but above all, the terrorist attacks of 11-9 awakened the interest of Brussels in the treatment of this new criminal activity, which in the USA has been described as “one of the crimes that is rising most rapidly⁶”, causing large-scale economic loss to financial entities and collateral losses for citizens needing to re-establish their identity.

No stranger to this criminal activity that was producing immense damage according to the alarming data from the *Federal Trade Commission* and the dramatic stories reported on in detail by the North-American press, the European Commission started to treat the threat more seriously. As many as three of its Directorate Generals (DG) -DG Internal Market and Services, the Joint Research Centre and DG Justice, Freedom and Security- undertook to study the problem from various perspectives: the first two centred on identity theft in the financial sector and on technological security measures, while the third covered more links with organized crime. In any case, it should be noted that in its first contact with this criminal activity, the Commission showed itself to be somewhat timid and preferred neither to speak specifically about “identity theft”,

6 COLE, S.A./PONTELL, H.N.: “Don't Be Low Hanging Fruit'...”, op., cit.

nor did it propose the possibility of describing the offence in either a broad sense, covering any type of fraud (financial, Social Security, etc.), or as a separate offence unconnected to its consequences (financial fraud due to forgery, for example), as the US regulations do. On the contrary, the approach it chose was to concentrate on one specific type –financial fraud- and to study the convenience of adopting preventive measures that would hinder the falsification of non-cash means of payment. Along these lines, the *Communication from the Commission of 1998*⁷ instigated the adoption of a joint action that would guarantee a legal definition in criminal law for all non-cash means of payment, punishable by effective, proportionate and dissuasive penalties in all Member States. The legislative proposal materialized with the approval of the Treaty of Amsterdam in the form of a Framework Decision in 2001⁸. Other documents followed the Communication which, despite making no mention of “identity theft”, kept the issue over illegally obtaining or appropriating data as the first phase of this crime very much in mind. In this sense, the *Resolution on the Communication 1998*⁹ in which the European Parliament urged the adoption of legislative or other measures consisting of improvements to identification methods and solvency in the issuing of credit cards by financial institutions, the use of a secure means of card delivery and encrypted data transmission at all times.

7 See, *Communication from the Commission to the European Parliament, the Council, the European Central Bank and Economic and Social Committee “A framework for action on combatting fraud and counterfeiting of non-cash means of payment”* [COM (1998) 395].

8 *Council Framework Decision, of 28 May 2001, combating fraud and counterfeiting of non-cash means of payment* [OJEU L 149, 2 June 2001].

9 *Resolution of the European Parliament on the Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and Europol - Preventing fraud and counterfeiting of non-cash means of payment* [OJ C 379/01, 7 December 1998].

Along with the legal definition of falsification of non-cash means of payment, the introduction of computer crime was established as one of the priorities in the fight against fraud committed with new technologies¹⁰, which had to follow the measures outlined in the *Convention of the European Union on Cybercrime, 23 November 2001*¹¹, the establishment of an effective regulation on data protection¹² (which can not, for example, be said of the USA) and, finally, cooperation between the public and the private sector¹³.

10 Proposal made thanks to *Council Framework Decision 2005/222/JHA, of 24 February 2005, on attacks against information systems* [OJEU L 69, 16 March 2005].

11 *Communication from the Commission: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*, p. 7 and *Commission Staff Working Document: Report on the implementation of the EU Fraud Prevention Action Plan on non-cash means of payment*, Brussels, 20 October 2004 [SEC (2004) 1264].

12 In part, already introduced in certain directives such as *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* [OJ L 281 of 23 November 1995]; and by the regulation in force at that time *concerning the processing of personal data and the protection of privacy in the telecommunications sector* [OJ L 24 of 30 January 1998], repealed by *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)* [OJ L 201 of 31 July 2002], modified in turn by *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* and by [OJ L 105, of 13 April 2006].

13 See *Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and EUROPOL Preventing fraud and counterfeiting of non-cash means of payment* [COM (2001) 11 final], p. 3 and *First Meeting of the Eu Forum on the Prevention of Organised Crime: Discussion Paper on the role of the private sector in the prevention of crime – a European perspective*, Brussels, 17/18 March 2001 (available in English at http://ec.europa.eu/justice_home/news/information_dossiers/forum_crimen/workshop/en/workshop3.pdf).

The view of identity theft as something close and intrinsically linked to other criminal activities which in themselves do not require separate attention emerged in 2003 and 2004. At this time, institutional documents started to appear which referred to identity theft as a particular problem¹⁴. The review of progress on the *Action plan 2001-2003*¹⁵ as well as the Communication, announcing 'A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment'¹⁶ highlight this activity as a new form of fraud and as a new threat. The plan takes a step forward by establishing as a recommendation the proposal for specific initiatives intended to prevent usurpation of identity in the EU¹⁷. The new actions plans fixed in both documents reveal that the Commission had promoted the debate on this matter and had revealed its intention to scrutinize the problem in greater depth. Evidence of this was the drafting of reports and the organization of seminars and workshops that were entrusted to specialist Ec bodies such as the *Joint Research Centre* or the *EU Fraud Prevention Expert Group*.

14 The first document that found in the course of this research in which express mention is made of "identity theft" is dated 27 May 2002, but it is a question written by a parliamentarian, Señor Cristiana MUSCARDINI, which does not directly refer to criminal Law and it only serves to ensure that the Commission report to the EP on research carried out by the Union on this matter. In the question, the regulation of Internet was suggested as an essential measure, at least in reference to security in the processing of personal data, given that the threat of data theft was global. See written question (only in Spanish) E-1476/02 of Cristiana MUSCARDINI (UEN) to the Commission, 27 May 2002.

15 *Commission Staff Working Document Report on the implementation of the EU Fraud Prevention: Action Plan on non-cash means of payment*, Brussels, 20 October 2004, p. 8 [SEC (2004) 1264].

16 Brussels, 20 October 2004, p. 3 [COM (2004) 679 final].

17 Bear in mind that in the case of documents written in Spanish and French the expression that is used is not "identity theft", but "usurpación de identidad [usurpation of identity]".

2. The consolidation of the discourse

The DG of the *Joint Research Centre* and more specifically the *Institute for Prospective Technological Studies* and the *Institute for the Protection and the Security of the Citizen*¹⁸ have, since 2003, led the research into "identity theft". The joint work of both institutes has produced two reports. The first, published in 2003, provides a general overview of *Security and Privacy for the citizen in the post-September 11 digital age*¹⁹. Of interest above all to what concerns us here is the warning of an increase in identity theft cases in the real and the virtual work, making it necessary to adopt acceptable safeguards of a more technological sort (use of biometric techniques, for example). With respect to criminal Law, the report notes the absence of specific criminal legislation on identity theft, although it does not see it as problematic as there are other criminal offences in which it can be subsumed²⁰.

The second report²¹ covers identity theft in particular and was presented at the *Seminar on identity theft*, held on February 2, 2004. It introduces

some of the most controversial questions that are ascribed to identity theft: on the one hand, the question of collateral damage to the victim (identity theft restoration), as the status of the consumer as a victim in cases of financial fraud is greatly debated as is the consideration of damages when defining a certain behaviour as an offence²²; on the other hand, there is the connection between identity theft and organized crime²³, in other words, between the misappropriation of data and use of false identities and aiding and abetting the commission of terrorist offences, trafficking in drugs, arms and human beings, etc. The report stresses the inexistence of a crime of these characteristics in the majority of member States, but once again appears to sidestep the debate on its introduction, remaining content with its punishment through other regulations such as cybercrime or the fraud²⁴. Thus, the idea is implicitly upheld that there is no specific injustice in "identity theft" that can not be covered by any of the more common and traditional criminal offences²⁵. The analysis is also relevant in this report on the role of firms. It identifies them as guilty or at least unwilling participants in identity theft due to the failure of their security systems. The identity thieves, the report concludes, often appropriate information that is stored in databases managed by firms that are not really conscious of

18 The *Joint Research Centre* was created in 1957 as a result of the EURATOM Treaty. Its main aim was to oversee nuclear safety and security in Europe. At present, it is a Directorate General of the European Commission under the European Commissioner for Research, Innovation and Science, Janez POTOČNIK. It has seven research institutes: *Institute for Reference Materials and Measurements (IRMM)*; *Institute for Transuranium Elements (ITU)*; *Institute for Energy (IE)*; *Institute for the Protection and the Security of the Citizen (IPSC)*; *Institute for Environment and Sustainability (IES)*; *Institute for Health and Consumer Protection (IHCP)* and the *Institute for Prospective Technological Studies (IPTS)*. For further information, see <http://ec.europa.eu/dgs/jrc/index.cfm?id=10>.

19 For example, the *Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE): "Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview"*. An executive summary is available at <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/20823-ExeSummaryEN.pdf>.

20 *Ibidem*, p. 32.

21 MITCHISON, N./WILIKENS, M./BREITENBACH, R./URRY, S.: *Identity Theft. A Discussion Paper*, European Commission, Directorate-General Joint Research Centre, 2004.

22 See in this volume the contribution by MAROTO CALATAYUD. On the same lines, see NIETO MARTÍN, A.: "Robo de identidad: Del fraude económico a las migraciones clandestinas", in *Jornadas sobre Derechos humanos y armonización internacional del Derecho penal en el 60º Aniversario de la Declaración Universal de los Derechos humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 19 and 20 January 2009. The video on the conference address is available at: http://v2.uclm.es/video.aspx?id_video=d76acfea-780e-419f-9ab6-144645c38be8.

23 MITCHISON, N./WILIKENS, M./BREITENBACH, R./URRY, S.: *Identity Theft...*, op., cit., p. 21.

24 This question is treated on two occasions on the same page. See MITCHISON, N./WILIKENS, M./BREITENBACH, R./URRY, S.: *Identity Theft...*, op., cit., p. 24.

25 In this respect, see MAROTO CALATAYUD for criticism on this volume.

the importance of investing in security²⁶. Consumers, therefore, are not the only ones that should take precautionary measures, so too should companies, with even greater reason, which store sensitive information that might be used to commit fraud of very different nature.

Towards the end of 2004, a change in leadership took place in the initiatives to study identity theft. The Commission continues to maintain a presence in each and every one of the proposals and lines of action. From now on, however, this will no longer be the work of the Joint Research Centre and the tasks will be moved to the DG Internal Market and Services, which will have the support of EU *Fraud Prevention Expert Group* (FPEG), which despite having been set up in the *2001 Action Plan*, did not assume a leading role until the creation of subgroup in 2004, specifically dedicated to identity theft²⁷. Representatives from national banking systems and the EU participate in the FPEG from banks, ministries and the central banks of the Member States, law enforcement bodies (including Europol and Interpol), the Central European Bank, retailers, consumer associations and network operators.

The emergent activity of the FPEG coincides with the adoption of a new *Action Plan (2004-2007) to prevent fraud on non-cash means of payment* by the Commission²⁸ in which the adoption of "Specific initiatives [that] should be undertaken to prevent identity theft in the EU²⁹" is a priority. "Com-

prehensive preventive measures" the Plan later points out³⁰. The definition of identity theft in its own right appears not to enter that category yet and, therefore, any reliance on criminal Law is still a long way off, although protected or juridically relevant interests start to define themselves around the strengthening or reinforcement of user confidence in the means of payment³¹. Indeed, all the measures in the report are directed at achieving that objective: the provision of satisfactory information on security to consumers, the use of the *European Network and Information Security Agency* (ENISA) as a coordinating body between payments providers and retailers, in order to improve their security systems against cybercrime, the creation of a *Single Payment Area in the EU* (SEPA) and the introduction of a single telephone number to report lost or stolen payment cards.

When therefore does the idea of harmonizing criminal legislation in the Member States arise and of obliging them to define identity theft as an offence, as well as punishing it with effective, proportionate and dissuasive sanctions? The idea was proposed for the first time at the "High Level Conference on maintaining the integrity of identity and payments", held in Brussels on November 22, 2006³² in the framework of the *Action Plan (2004-2007)*, and jointly organized by the DG Internal Market and Services and the DG for Justice, Freedom, and Security. Some of its speakers referred to the need to establish common definitions for identity theft³³ and others went even further, to the point

26 *Ibidem*, p. 27.

27 The group was created by the Commission through the *Action Plan 2004-2007*. It is made up of public and private institutions with an interest in fraud prevention, such as banks, public administrations, Europol, consumer associations, networks providing services, etc. For more information, see http://ec.europa.eu/internal_market/fpeg/index_en.htm.

28 *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment*, Brussels, 20 October 2004 [COM (2004) 679 final].

29 *Ibidem*, p. 9.

30 *Ibidem*, p. 10.

31 On the legal right that pertains to identity theft, see NIETO MARTÍN, A.: "Robo de identidad: Del fraude económico a...", *op. cit.*

32 All information concerning this conference may be consulted *online* at http://ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/index_en.htm.

33 RAVOET, G.: "The Impact of Fraud and Identity Theft on Banking and Financial Systems", High Level Conference on maintaining the integrity of identity and payments", held in Brussels, 22 November 2006, p. 9.

of approaching the problem through the introduction of specific offences relating to identity theft in the digital world³⁴. Nevertheless, not everybody voiced opinions along the same lines, among which the opinion of the General Prosecutor in Bamberg, Heinz-Bernd WABNITZ, who considered that the existing regulations in (at least German) national Law on cybercrime and traditional fraud were sufficient to cover all circumstances of identity theft³⁵. In this conference, the Commission also made known its intention, as a prior step to ensure the success of any community legislative reform and to pre-empt criticism, to draft a comparative Law study on criminal legislations in Member States with respect to identity theft³⁶.

Months after holding the conference, the Commission released a Communication entitled "Towards a general policy on the fight against cybercrime"³⁷. This is the first institutional document in which the imminent arrival of identity theft in the Member States is envisaged as a separate offence³⁸ and to which, moreover, legislative har-

monization is linked; hardly surprising given the trajectory of the Union in criminal law, towards the improvement of mutual cooperation in substantive criminal matters without having taken account of the criticism set out by the doctrine on the functional relationship between substantive and procedural criminal law³⁹. It is pointed out on page 8 of the Communication that "(...) EU law enforcement cooperation would be better served were identity theft criminalised in all Member States". At that point, the Commission began to consult the different parties on the convenience of legislating in that direction.

The impact assessment report prior to the Communication had already warned of the inconvenience involved in the harmonization of criminal legislation on identity theft, indicating as fundamental obstacles the difficulty of adopting a criminal law in accordance with the legal traditions and practices of the member States and the risk of criminalising non-damaging activities that would be incompatible with respect to the criminal principle

34 VULPIANI, D.: "Digital identity theft by the use of the Internet", High Level Conference on..., op., cit., p. 6: "It is necessary to envisage crime typologies expressly fit for digital identity thefts and all UE countries should provide for appropriate strict measures".

35 WABNITZ, H.B.: "How to make investigation more effective – The experience of a national magistrate", High Level Conference on..., op., cit., p. 4: "Die Schaffung eines eigenen Straftatbestandes erscheint daher nicht als erforderlich".

36 *Draft Minutes 11th Meeting of the Fraud Prevention Expert Group*, 28 November 2006, Brussels, 12 December 2006 MFS D (2006).

37 *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Towards a general policy on the fight against cyber crime*", Brussels, May 22, 2007, [COM (2007) 267 final].

38 The germ of this new policy to combat cyber-crime through the preparation of specific legislative measures has already advanced, nevertheless, in the *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - On fighting spam, spyware and malicious software*, Brussels, 15 November 2006, p. 12 [COM (2006) 688 final]: "The Commission (...) introduce new legislative

proposals at the beginning of 2007 that strengthen the rules in the area of privacy and security in the communications sector and present a policy on cyber crime".

39 In general, KAIIFA-GBANDI, M.: "Memorandum", in *Select Committee on European Union – Written Evidence*, 7 April 2008, §D and KAIIFA-GBANDI, M./CHATZINIKOLAOU, N. et al.: "The FD on combating trafficking in human beings: Evaluating its fundamental attributes as well as its transposition in Greek criminal law", in WEYEMBERGH, A./SANTAMARÍA, V. (ed.): *The evaluation of European criminal law*, op., cit., p. 187. As a concrete example, see NIETO MARTÍN, A. (ed)/MAROTO CALATAYUD, M./MUÑOZ DE MORALES ROMERO, M.: "El fraude mediante tarjetas de pago. Un estudio de Derecho comparado", p. 12 (manuscript). In this report the fact that article 6 of *Framework Decision combating fraud and counterfeiting of non-cash means of payment* orients penalties not towards the importance of the legal right, but towards possible judicial cooperation and especially extradition. VOGEL, J. also adopts a critical voice: "Wege zu europäisch-einheitlichen Regelungen im Allgemeinen Teil des Strafrechts", in *Juristenzeitung*, 1995, p. 336 and DANNECKER, B.: „Strafrecht der Europäischen Gemeinschaft", in *Juristenzeitung*, 1996, p. 873.

of harm or prejudice⁴⁰. For this reason, legislative harmonization in the near future is not advised and the report recommends the adoption of non-legislative measures tending to facilitate cooperation between public and private authorities, and to guarantee better application of the legal regulations that are already in force. Rejection of harmonization is provisional, because it is made quite clear in the assessment that if these non-legislative measures were to fail, criminal legislation could be considered; the nature of which is not specified, but left open for discussion⁴¹. The approach that implicitly considers the principle of *ultima ratio* of Criminal law should at least be assessed, although I do not believe that was the Commission's intention, as prior to considering the punishment, other alternatives are considered.

The advisability of adopting specific criminal measures on identity fraud was debated with greater or lesser force in successive conferences held in 2007⁴², but without a doubt it was the conference organized under the Portuguese European Presidency⁴³ which awakened most interest from the point of view of our discipline. Taking a previous report from the FPEG⁴⁴ as a reference, the general

idea that dominated throughout this event was the need to have specific criminal legislation on identity theft as a prior step to guaranteeing effective judicial cooperation⁴⁵. Nevertheless, opinions were aired that compared the system offered by the *Council of Europe Convention on Cybercrime*⁴⁶ and, its near replica at a European level, the *Council Framework Decision on attacks against information systems*⁴⁷. They underlined that the fight against identity theft did not necessarily have to begin with the North American approach according to which the use of another person's means of identification is punishable as a separate criminal offence. The contribution by M. GERCKE is of great interest on this point, who analyzing the provisions of the Convention and, also indirectly those of the Framework Decision, sowed reasonable and serious doubts with regard to the need to introduce a separate criminal offence for identity theft⁴⁸.

The Convention, ratified by more than half of all Member States⁴⁹, obliges the criminalisation of a series of behaviours that have a strong relation to two of the phases that are basically constituted by

40 *Commission Staff Working Document - Accompanying document to the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the Fight against Cyber crime - Impact Assessment Report*, § Assessment of policy options, General policy option 2. General legislation [SEC (2007) 642 final].

41 *Ibidem*, in fine.

42 A list of conferences on identity theft and related themes organized throughout 2007 may be consulted in the *Draft Agenda. 13th Meeting of the Fraud Prevention Expert Group*, 19 December 2007 (Brussels, draft 3 December 2007 MFS D (2007) and in a more exhaustive way in a subsequent version, 24 January 2008 (both texts available at http://ec.europa.eu/internal_market/fpeg/meetings_en.htm).

43 All the documents mentioned in relation to this conference are available *on line* at <http://www.idfraudconference-pt2007.org/>

44 See *Report on Identity Theft/Fraud*, Fraud Prevention Expert Group, Brussels, 22 October 2007, p. 35 (only available in English).

45 See, for example, the conference address of OZAKI, K.: "Identity Fraud and Theft: An overview of the problem and its criminal diversity", p. 11: "(...) proper legislation to criminalize identity-related crime is essential to any effective fight against such crime" and the final report "European Identity Systems: A Comparative Study", Ministry of the Interior (Ministerio da Administração Interna), Internal Security Coordinating Office (Gabinete Coordenador de Segurança), Portugal, Lisbon, 7th March 2009, pp. 28-29.

46 *The Convention on Cybercrime of the Council of Europe*, Budapest, 23 November 2001 (STE n. 185).

47 *Council Framework Decision 2005/222/JHA of 24 February 2005, on attacks against information systems* [OJEU L 69, 16 March 2005].

48 GERCKE, M.: "Internet-Related Identity Theft: A Discussion paper", pp. 14-20.

49 Up until 9 June 2009, the Convention has been ratified by a total 15 Member States: Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Romania, Czechoslovakia and Slovenia. Source: <http://conventions.coe.int/TreatyCommun/QueVoulezVous.asp?NT=185&CM=8&DF=6/9/2009&CL=ENG>.

identity theft: illegal appropriation of data and their fraudulent use⁵⁰. With regard to the first phase, the text of the Convention for the Council of Europe envisages the offence of illegal access to the totality or to one part of the information systems (including, therefore, the data stored in an information system)⁵¹, behaviour commonly known as “hacking”; the illegal interception of transmissions, including electromagnetic emissions produced by a computer system (a behaviour that is not contemplated in the FD)⁵²; data interference (in particular damage, alteration or deletion of information)⁵³; system interference (hindering without right of the

functioning of a computer system)⁵⁴; the misuse of devices⁵⁵: distribution of tools for the purpose of hacking or computer *passwords* with the intent to commit offences and computer fraud⁵⁶ (neither are the latter behaviours envisaged in the FD).

The first behaviour described –*hacking or illegal access*– is drafted in such broad terms that it also includes access to a computer system to obtain information related to a person’s identity⁵⁷, as a consequence, this criminal definition would cover the

50 The intermediate phase, which relates to trafficking in personal identifying information or with false documents, is often subsumed in the stage of illegal data acquisition, given that the same person that acquired the data and, subsequently commercialized it, for example, by selling it to organized criminal gangs, had illegally obtained it.

51 Article 2 of the Convention – Illegal Access: “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.” and similarly, article 2 of the FD.

52 Article 3 – Illegal Interception: “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.”

53 Article 4 – Data Interference: “1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. 4 FD.

54 Article 5 – System interference: “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.” and similarly article 3 FD.

55 Article 6 – Misuse of devices: “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.”

56 Article 7 – Computer-related fraud: “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches”.

57 GERCKE, M.: “Internet-Related Identity Theft...”, op., cit., p. 14.

phase prior to the identity theft, which is the illegal appropriation of data⁵⁸. The legal definition, for its part, of damaging, deletion, deterioration, alteration and suppression of computer data can also be used to prosecute identity thieves, as on occasions the theft of the data is often accompanied by the use of malicious software (worms and virus)⁵⁹. The same may be said with respect to the offence of system interference, whose scope of application also includes those cases in which the appropriation of data is linked to serious interference in a computer system.

The Convention also contemplates the possession and distribution of certain devices or dangerous tools (including computer programmes) and the production and distribution of computer passwords and similar data that can be used to gain illegal access to computer systems (article 6). This regulation has been discussed at great length because it entails too much of an advance on criminalisation. Thus, SIEBER warns that these types of preparatory crimes are not usually present in national criminal law in view of the unpredictability of the specific circumstances in which codification or distribution of these types of programmes could be carried out, for which reason the Convention limits the criminalisation of these circumstances to those in which the device is objectively designed for the purpose of committing an offence and requiring, moreover, intent to commit specific offences⁶⁰. For the purposes of this paper, the relevant point is that this precept covers the circumstances in which the appropriation of identity-related information has come about after the production, sale, appropriation for its use, importation, diffusion or any other

form of making the device available, including a computer programme principally designed or adapted for that purpose, or a password, an access code, or similar computer data that provide access to all or part of the computer system⁶¹.

In a similar way to the forgery of documents, the Convention under article 7, seeks to oblige the States party to define computer crime, understanding it as the input, alteration, deletion or suppression of computer data that results in non-authentic data, with intent to have such data accepted or used for legal purposes as if they were authentic data. This provision covers the forgery of electronic documents and, in particular, the forgery of emails that are used as *phishing*⁶².

In relation to phase 2 of identity theft, which is the fraudulent use of illegally obtained data, article 8 of the Convention requires the criminalisation of acts "when committed intentionally and without right", which cause "loss of property to another person by: a) any input, alteration, deletion or suppression of computer data, b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person", which covers the cases in which the fraud consists of the use in the network of bank cards⁶³.

In view of the above, it may be appreciated as a preliminary difference with respect to North-American criminal policy that neither the Convention nor the FD therefore defines the appropriation or use of identity data as an offence. The Convention does not cover all acts that aim to appropriate personal data nor their subsequent use (for example, obtaining data through non-electronic means⁶⁴). However, for

58 *Ibidem*, p. 15.

59 See *Combating Identity Theft – A Strategic Plan*, US President's Identity Task Force, 2007, p. 66 (available at: <http://www.idtheft.gov>).

60 SIEBER, U.: "Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law", in DELMAS-MARTY, M./PIETH, M./SIEBER, U. (dir.): *Les chemins de l'harmonisation pénale/Harmonising Criminal Law*, Société de Législation Comparée, 2008, p. 143.

61 GERCKE, M.: "Internet-Related Identity Theft...", op., cit., p. 17.

62 *Ibidem*, p. 18.

63 *Ibidem*, p. 19.

64 RUSCH, J.J.: "Cybercrime and Identity Fraud and Theft: A United States Perspective", *Presentación power point a la Conferencia de la Presidencia europea de Portugal*, dia.

the acts that do fall within its scope of application, the appropriation and use of information is not limited to data of a personal nature. Legal treatment on each side of the Atlantic is totally different; whereas the Convention prefers to protect a set of different legal interests, such as the integrity of a computer system, the US approach is inclined towards protection of the integrity of identity data⁶⁵.

The *Communication on follow up of the 2004-2007 Action Plan* linked the advisability of following the same road as the U.S.A. to the results obtained from a prior study on criminal legislation in the Member States⁶⁶. As a result, an invitation to tender was published in 2007 to carry out a "Comparative study to evaluate the need for instruments to combat organised crime activities related to identity theft in the EU Member States⁶⁷". The adjudication decision was planned for the end of that same year but was delayed until autumn 2008⁶⁸. A little later, the Commission announced the cancellation of the project for administrative reasons⁶⁹. Without a doubt it is a lost opportunity, which could have appreciated whether, even in the absence of a specific criminal provision on identity theft, the majority of States had the tools to prosecute such offences through, for example, fraud or computer

forgery. It could also have examined whether the facilities for criminal prosecution, in other words the functional nature of substantive criminal Law with respect to procedural Law, was a sufficiently important interest to opt for the criminalisation of such a controversial offence. The States that have opted for identity theft as a separate criminal offence usually argue that it is easier to prove a crime of identity theft than other offences which may be committed afterwards with the stolen data⁷⁰, given that the criminals' use of a false identity more than complicates the search for and the detention of the offender. I do not believe that this is sufficient reason in itself. In any case, the withdrawal of the study by the Commission appears to have ended, at least provisionally, criminal harmonization of identity theft as a priority or target in the Area of Justice, Freedom and Security.

III. Competential Strategies

Prior to the entry into force of the Treaty of Lisbon, the competential bases of the Union to adopt a harmonizing criminal regulation in matters concerning identity theft could be two: either under the First Pillar, former article 95 TEC (actual art. 114 TFEU) relating to the approximation of laws with the aim of establishing or ensuring the functioning of the internal market, or within the framework of the Third Pillar, through the old article 31.1 e) TUE, under which the Union has the authority to adopt measures that establish minimum rules relating to the constituent elements of criminal acts and to penalties in the fields of organized crime, terrorism and illegal drug trafficking. The differences between using one or another legal foundation would have been considerable, not only at a judicial level (possibility of submitting appeals on the grounds of non-compliance) and procedural (procedural by co-decision/procedural consultation), but also due to

positivas nº 13 and ff. (available at: <http://www.id-fraudconference-pt2007.org/cms/files/programa/PFL47347a703f84b.pdf>)⁶⁵ GERCKE, M.: "Internet-Related Identity Theft...", op., cit., p. 20.

66 *Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan*, Brussels, 22 April 2008 [SEC (2008) 511]. Only available in English.

67 Invitation to tender 2007/S 120-146524. Available at: <http://ted.europa.eu/udl?uri=TED:NOTICE:146524-2007:TEXT:EN:HTML>

68 See *Commission Staff Working Document Annex to the Communication from the Commission to the Council and the EP: "General overview of instruments and deadlines provides for in the Hague Programme and Action Plan in the fields of Justice, Freedom and Security for 2007"*, Brussels, 2 July 2008 [SEC (2008) 2049], p. 22

69 See Doc. nº 21637-2009, in Supplement to the OJEU, 24 January 2009.

70 GERCKE, M.: "Internet-Related Identity Theft...", op., cit., p. 20.

the type of legal instrument that is used (directive/framework decision) and the class of arguments to support its adoption (improvement of the functioning of the internal market/improvement of judicial cooperation in criminal matters).

With the latest modification of the constituent treaties, the competential panorama is greatly simplified, such that at present the only possible legal base would be art. 83 TFEU. In this respect, it is highly likely that future community criminal interventions in the field of identity theft would be presented as "a complement, as a logical evolution"⁷¹, both of the *Council Framework Decision on attacks against information systems* examined earlier and of the *Council Framework Decision combating fraud and counterfeiting of non-cash means of payment*⁷². As a consequence of the latter, criminal regulation of identity theft would be limited to a financial context. On the contrary, as an accessory rule of the *Council Framework Decision on attacks against information systems*, the criminal definition could cover many areas and approach the US regulation: social security fraud, defrauding the treasury, etc. In both cases, the Commission would certainly use, as an argument to intervene, the all-too-well-known reason of fighting more effectively against organized crime as a priority objective for the consolidation of a European Area of Freedom, Security and Justice, and it would find support in the social concern generated by the increased likelihood of terrorists and leaders of networks that traffic in drugs, arms or humans managing to obtain and use identities to hinder investigations on the part of public authorities. It remains to be seen whether the community regulation will cover identity theft undertaken without the help of new technologies, both in the phase of the illegal appropriation of data and in its commercialization, transfer or use, as the cases in which the use of new information technolo-

71 NIETO MARTÍN, A.: "Robo de identidad...", op., cit.

72 *Council Framework Decision 2001/413/JHA, of 28 May 2001, combating fraud and counterfeiting of non-cash means of payment* [OJ L 149, 2 June 2001].

gies are not present are less extensive and are hypothetically less likely to occur at a transnational level. In consequence, there would not be such a pressing need, from the perspective of the subsidiarity principle in article 5 §2 TFEU⁷³, to regulate such a conflictive legal definition at a community level.

IV. Conclusions

The contents of this contribution demonstrate how once again the USA acts as a harmonizing force on law in general and criminal law in particular. We have seen it in economic contexts such as money laundering and now also with identity theft. It is true that the definition of such behaviour at a community level has still not taken place, but the debate has started and is unlikely to end soon. The most surprising aspect is that such a conflictive legal definition is going to be imported into a society, that of the European Union, which does not have the same characteristics as the North-American society. Thus, for example, the Union has very powerful legislation on data protection that does not exist on the other side of the Atlantic. Neither should the generalized rejection in the USA of official identification documents similar to the Spanish national identity document go unremarked, it having on the contrary chosen administrative documents (social security number) as an identification system, which run a greater risk of misappropriation and subsequent misuse. Finally, United States culture is heavily indebted and dependent on consumerism: a tendency also experienced in Europe, but which is not –at least not yet- as aggressive or as obvious⁷⁴. ■

73 "Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level».

74 On this marked differences, see above the contribution by Manuel MAROTO CALATAYUD.

