Dr. Roberto Flor
Faculty of Law
University of Verona - Italy

Fraud, Computer-related fraud and Identity-related fraud

New forms of offences, through the use of new technologies, to the European Union's financial interests or to the integrity of the computer systems of the European institutions or to the confidentiality of data

by

Roberto Flor

Faculty of Law – University of Verona

Contents

Dr. Roberto Flor
Faculty of Law
University of Verona - Italy

1. Introduction

This paper is an abstract of the study, ordered by the European Commission and the European Anti-Fraud Office, that consists in an analysis, through an empiric survey, of the behaviours of fraud and other illegal activities that threathen the European Union's financial interests, in particular carried out through the new technologies: computer-related fraud and forgery (presentation of false information or false documents or statements), illegal access to data and information systems, cyberlaundering, identity-related fraud and phishing attacks.[1]

2. The results of the empiric analysis

From the empiric analysis and from the study of the reports of other international institutions it is possible to draw, in a preliminary way, the following information:

1. the difficulies in collecting common definitions and terms for the identifiction of phenomena having a similar structure;
2. the difficulty in collecting empirical data for reasons connected to different factors (among which the nature of the data stored in the EU's institutions computer systems, that need protection and discretionality also with regard to possible previous attacks).

From the **results of the comparative analysis**, we can distinguish on a systematic plan different forms of attack carried out through the new technologies, that can be subdivided, according to the general category into which the offence can be included, in the two following groups:

1. computer crimes ("in the literal sense", "in senso proprio")and c ybercrimes, the typical mean of commission of which is connected to computer technology, or the passive object of the conduct of which has a "technological-computer" character (data, software, computer systems etc.): let's consider, for example, illegal access or computer related fraud;
2. traditional computer crimes ("in senso improprio"), formed by common crimes that can be committed also through the use of computer instruments, but that lack a typical requisite or element necessarily involving computer technology, and that for this reason might also not be carried out in the cyberspace*:* for example common fraud and fraud against the interests of the EC.

At a phenomenological level, on the contrary, we can subdivide the **criminal behaviours**

a) with regard to the **direction or target** of the offence:

1. forms of direct attack/offence, meaning new forms of aggression, through the new technologies, to the EU's financial interests (for example fraud against the interests of the EC carried out through computer systems) or to the integrity of computer systems or to the confidentiality of data of the

[1] The report "*New forms of offences to the Community's financial interests committed through the Information technologies in a comparative perspective*" - written by the research unit of the Faculty of Law of Verona, *New Technologies Criminal law area*, under the scientific coordination of Prof. Lorenzo Picotti, full professor of Criminal Law, University of Verona (edited by R. Flor, ©2009, Verona, Italy) - is still unpublished.

European institutions (illegal access, reproduction of web pages, virus or malware attacks to computer systems of the European institutions);

2. forms of indirect attack/offence, having a preparatory or instrumental role with regard to the achievment of the final objective pursued by the perpetrator of the criminal offence (for example the acquisition of personal data, confidential information or passwords, with the aim of submitting an unauthentic application for obtaining grants for other activities) or constituting activities following the commission of a crime (and particularly money laundering or tampering with the traces of a crime).

b) with regard to the **perpetrators** of the offences:

1. single natural persons, also associated
2. legal persons, institutions or associations, irrespective of whether they are in a leading or in a subordinate position

c) with regard to the **origin** of the attacks or of the violation of rules issued by European sources or having an organizational character

1. *insider* – for example outside communications of confidential data concerning an investigation via e-mail or via other communication devices;
2. *outsider* – for example unauthorized access to the computer system of an institution through Internet and/or the use of malware.

Thus, shortly, the phenomena monitorized represent new or partially new forms of offences against the Union's financial interests (for example computer-related fraud with the aim of obtaining European grants), or elements of more complex criminal phenomena, yet only indirectly damaging such interests (for example identity theft with the aim of subsequently apply for European grants and funds). They can be summarized as follows.

Forms of direct attack	
Fraud and Fraud to EU	Artifices or deceptions carried out through the use of computer instruments or communication tools with the aim of obtaining undue allocations, also through the use or the presentation of false or incorrect declarations and papers, or through the non-disclosure of information (for example via e-mail)
Identity abuse	Illicit use of another person's identity or of a false identity, both in an electronic form and through the use of identity papers (for example through authentication credentials in order to have access to restricted areas)
Computer related fraud*	The causing of a loss of property to another person by: any input, alteration, deletion or suppression of computer data any interference with the functioning of a computer system, with the fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Data and system inteference *	The damaging, deletion, deterioration, alteration or suppression of computer data without right and the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data
Computer related forgery**	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.
	Any wilful act or omission concerning the use or presentation of false, incorrect or incomplete declarations or papers, and the ensuing illicit perception or retention of funds issued from the general budget of the European Community or from the budgets managed by the European Community or on its behalf.
Illicit treatment of confidential data	Violation of the regulation in the matter of protection of personal data (including all activities carried out without the authorization of the legal owner or violating a rule, such as the communication, the diffusion, the acquisition, the filing and the storing of data)
Identity related fraud	Abuse of the identity illicitly or deceptively acquired with the purpose of obtaining goods or services, or anyway with the purpose of carrying out criminal activities aiming at obtaining a profit or/and at causing a property loss to other persons. The phenomenon is thus composed by different elements, among which identity abuse and identity theft.

* definition adopted on the basis of what is provided by the Convention on Cybercrime.
** definition adopted on the basis of what is provided by the Convention on Cybercrime and by the PIF Convention.

Forms of indirect attack

Identity theft	The seizing, without authorization or in a fraudulent way, or the "theft" or illicit acquirement, of another person's confidential data, concerning a natural person, dead or alive, or a legal person.
Illicit money tranfers through the web	Money laundering committed through the use of computer instruments, also through credit transfers or funds transfers.
Investment fraud or Business fraud**	*Investment Fraud* - Deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains. *Business Fraud* - When a corporation or business knowingly misrepresents the truth or conceals a material fact.
Illegal access* (hacking)	See above, as a preparatory activity for obtaining data and information useful for the commission of another offense
Data interception*	See above, as a preparatory activity for obtaining data and information useful for the commission of another offense.
Data and system inteference*	See above, as a preparatory activity for obtaining data and information useful for the commission of another offense, or as a consequence of the crime committed with the aim of erasing the traces of the crime.
Misuse of device*	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, an access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the 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…(see art. 6 CoC).
Fraud to the certifier of electronic signature	False declaration or statement to the certifier of electronic signature on one's own or other persons' identity or personal capacities with the aim of committing further offences (for example to apply for a grant).
Illicit treatment of confidential data	Violation of the regulation on the matter of protection of confidential data (including the activities carried out without the authorization of the legal owner and violating a rule, such as the communication, the diffusion, the acquisition, the storing and filing of data, also as an activity preparatory to obtain data and information useful for the commission of another offence)

* definition adopted on the basis of the Convention on Cybercrime.
** definition drawn by the *IC3 crime report*

We have detected the "categories" of criminal behaviours belonging to the new forms of direct and indirect offence to the financial interests of the European Union or to the integrity of computer systems of the European institutions or to the confidentiality of data, and to the use of computer systems of the European Union with the purpose of committing an offense.
In the second part we considered the regulations in force in some European States, comparing them with the European and international sources on the matter.

3. Fraud, Computer-related fraud and Identity-related fraud

The spreading, the growing and progressive changes of the phenomena connected to computer-related fraud and to identity-related fraud, and among them identity abuse and identity theft, mark the passage from the phase of the so-called computer crimes to the phase of cybercrime, which finds in the cyberspace an ideal environment for the commission of many, different and new forms of offences.
This paragraph will have to take into account not only traditional computer crimes, but also non-traditional crimes, and therefore common fraud (meant *strictu sensu*) committed through the misuse of computer devices. In fact, the national legislations we have taken into account lack a specific normative discipline considering the phenomenon from a unique point of view.
This latter manifests itself not only through unauthorized manipulations carried out through "the damaging, deletion, deterioration, alteration or suppression of computer data without right" or through "the serious hindering without right of the functioning of a computer system", but also through the commission of traditional crimes, that may be carried out through "technological devices".
The protection of the financial interests of the European Communities has been strengthened, in the fight against fraud, by the Convention on the Protection of the Financial Interests of the European Communities (also known as PIF Convention), adopted on 26 July 1995, aiming at harmonizing national regulations and at securing communitarian finances an adequate protection level.
Article 1 of the Convention gives a definition of "Fraud affecting the Community's financial interests" wide enough to include "any deliberate omission" and "the presentation of false, incorrect or incomplete statements or documents", the illicit retention or misappropriation of paid out funds, as well as a number of "condotte di evasione" (among which "the use or presentation of false, incorrect or incomplete statements or documents" resulting in the reception or the illicit retention of funds from the general budget of the European Communities or from budgets managed by the European Communities or on their behalf; non-disclosure of information in violation of a specific obligation, resulting in the same effect; the "misuse of such funds for purposes other than those for which they were originally granted"), regardless of the use, as *typical mean*, of computer technologies, or of having as a *passive object* their "products" (data, software, computer systems).

Such means and object can nevertheless constitute en essential element of the actual commission of the criminal offence and, hence, they can be assimilated to the direct forms of aggression to said interests.

The structure of the fraud is, in fact, "totally assimilated also with the purpose of preventing fraud against the European Communities, and the only differentiating element is represented by the peculiar nature of the act of financial disposition that, we must remember, must consist in a subsidy, a grant, a loan or a similar allocation, granted or allocated by the European Communities".[2]

Notwithstanding the ratifications of the "PFI instruments" (including, besides the Convention, also two annex Protocols of 1996 and of 1997), the target of an actual harmonization has still not been satisfactorily achieved in this area, and it appears more and more difficult to be achieved now that the European Union has been "enlarged" to 27 Member States[3].

With regard to the **Identity related-fraud phenomenon**, the analysis of which can be carried out including also computer-related fraud, the legislations of the Member States of the European Union **lack** a common legal and/or criminological definition of "identity theft" and of "identity fraud"[4]. Moreover, at the criminological level, and in the different States, we find out that different meanings are attributed to such terms, that are sometimes used as synonymous or assimilated to the general category of "identity crime".

The definition of identity related-fraud is connected to the wider phenomenon of the unauthorized use of personal data in order to obtain goods or services by fraud, or anyway in order to carry out fraudulent activities with the intent of procuring an unauthorized economic benefit for the person committing the offence or for a third party**,** and/or of harming another person, even through phishing techniques[5].

The criminological definition of the identity-related fraud phenomenon has some elements in common with the legal definition of "fraud against the interests of the European Communities", that may include, among its phenomenological elements, activities preparatory to the presentation of false documents; such activities are not typified as specific means for the commission of the criminal offence, but they can become actual means in case computer documents are used, thus becoming forms of direct aggression.

---

[2] MUSCO, *Frodi comunitarie*, in FERRÉ OLIVÉ, JUAN CARLOS (ed.), *Fraude de Subvenciones Comunitarias y Corrupción: Delitos Financieros, Fraude y Corrupción en Europa*, Salamanca, 2002. Vol. I.

[3] See the *COMMISSION STAFF WORKING PAPER - Annex to the SECOND REPORT FROM THE COMMISSION - Implementation of the Convention on the protection of the European Communities' financial interests and its protocols - Article 10 of the Convention {COM(2008) 77 final}*., p. 8 ff.. As to the Italian legal theory see the wide analysis by PICOTTI, *L'attuazione in Italia degli strumenti dell'Unione europea per la protezione penale degli interessi finanziari comunitari*, in *Rivista trimestrale di diritto penale dell'economia*, 2006, p. 615 f.

[4] The lack of definition has been pointed out by FLOR, *Identity related-fraud e diritto penale: un approcio comparatistico nella prospettiva di riforma dei trattati europei*, in Picotti L. (ed.), I*l diritto penale nella prospettiva di riforma dei trattati europei. Diritto penale europeo e protezione degli interessi finanziari dell'Unione Europea* (2009); FLOR, *Phishing, Internet related-fraud, identity theft:* nuove forme di criminalità *on line*, in Picotti L. (ed.), *Quaderni per la riforma del codice penale. Tutela penale della persona e nuove tecnologie*, Cedam (2009) and FLOR*, Phishing, identity theft* e *identity abuse*: le prospettive applicative del diritto penale vigente, in *Riv. it. dir. proc. pen*., 2007, 899, with appropriate references.

[5] Phishing is commonly defined as a social behaviour aiming at acquiring sensitive personal information on a person's habits and way of life with the intent to access on-line financial or bank services, "virtually" impersonating the legal owner of the identity data (FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007, 899 ff.).

We have considered the **Italian, German, French, Spanish and Romanian criminal-law systems**; Romania has recently introduced criminal laws consistent with the provisions of the Convention on Cybercrime and therefore it represents a model of good practice[6].

4. Provisional conclusion: results of the comparative analysis

The legislation of the States monitored in this research have no specific crime for phenomena such as identity-related fraud; however, there exists a large number of criminal provisions covering the "phenomenological element" and the phases of commission of the offences.

The Italian and Spanish legislations, in particular, is marked by a multiplicity of crimes that might (ipothetically) be appliable[7].

The French legislation, lacking a specific rule in the matter of computer-related fraud, provided (L. 88-19/1988) the special crime of "forgery of computer-produced documents", later abrogated by the new Code in 1992 as the crime of computer-related forgery is assimilated to the common crime of forgery (in general) for the wide concept connected with its object: forgery may concern both "any written document" and "any other support of the expression of thought" (see article 441-1 Code Pénal); so, also computer-produced documents.

Fraud through computer tools is instead punishable after article 313-1 Code Pénal, owing to the width of the forms of commission expressed by the words "manoeuvres frauduleuses".

In the German Criminal Code, article 263a StGB, on the contrary, expressly provides the crime of *computer-related fraud*, consisting in harming another person or other persons by influencing the result of data processing operations through an incorrect configuration of a programme, the incorrect or incomplete use of data, the unauthorized use of data, or other unauthorized interventions on the course of events (for example, modifications, deletion or erasing of data)[8]

---

[6] See the discussion papers of the Conference "**Octopus Interface 2008**", in http//www.coe.int. See also GERCKE, *Internet-related Identity theft* (ver. 22.11.2007, edited 17.05.2008).

[7] FLOR, *Phishing, Internet related-fraud, identity theft*, cit. and FLOR, *Identity-related fraud e diritto penale,* cit.; FLOR, *Phishing, Identity theft e Identity abuse*, cit.; CAJANI, *Profili penali del* phishing, in *Cass. pen*., 2007, 2294 ff.; CAJANI, COSTABILE, MAZZARACO, *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008. About Spain see: FERNÁNDEZ TERUELO, *Respuesta penal frente a frau cometidos en Internet: estafa, estafa informática y los nudos de la red*, in *Revista de Derecho Penal y Criminologia*, 2007, 217 ff.; HERRERA MORENO, *El Fraude Informático en Derecho Penal Español*, in *Actualidad Penal*, 39, 2001, 925 ff.; LÓPEZ ORTEGA, *Internet y derecho penal*, ed. I, Madrid, 2002; PALOMINO MARTÍN, *Derecho penal y nuevas technologias*, Valencia, 2007 (cited by FLOR, *Identity-related fraud e diritto penale,* cit.).

[8] ERNST, *Das neue Computerstrafrecht*, NJW, n. 37, 2007, 2661 ff.; HILGENDORF, *Informationstrafrecht und Rechtsinformatik*, Logos Verlag, Berlin, 2004; ID., *Die Neuen Medien und das Strafrechts*, ZStW, 2001; HEINRICH, *Aktuelle Probleme des Internetstrafrechts*, in Humboldt-Forum-Recht, 11/2006. See SIEBER, *Liability for On-line Data Bank Services*. Information Technology Law Series (3), I.R.I. – Managing & Planning Organization of the High Council of Informatics, Teheran 2005/2006. See also GERCKE, *Phishing and Identity Theft*, in CR 2005, 598 und ID., *Die Strafbarkeit von "Phishing" und Identitätsdiebstahl - Eine Analyse der Reichweite des geltenden Strafrechts*, in CR 2005, S. 606 ff.; HANSENS, *Sfrafbarkeit des Phishing nach Internetbanking-Legitimationsdaten*, Hamburg, 2007, 13 ff. and 47 ff. On German doctrine, that not always uses this distinction, see STUCKENBERG, *Zur Strafbarketi von „Phishing"*, in ZStW, 2007, 878 ff.; BORGES G., *Rechtsfragen des Phishing. Ein Überblick*, in NJW, 46/2005, 3313 ff.

Moreover, the German legislation provides the crime of fraud against grants (ex § 264 StGB - *Subventionsbetrug*), applicable in the abstract to the above mentioned phenomena, in case all the constituting elements exist; such are the cases in which, for example, false information supplied to the institutions/bodies that supplies the funds, concern personal data of the applicant who has previously been the victim of identity theft. In such cases criminal behaviour have an independent criminal relevance, but they can also be considered as "elements" or "components" of a wider phenomenon, such as identity-related fraud.

With regard to the latter (meant as form of commission of a "fraud against the EU's interests", especially if its phenomenological elements concern not only those activities preparatory of the presentation of false documents, but consist a form of achievement of a "communitarian" fraud), we need to point out that Germany is considered among the States that have strictly implemented the dispositions of the PIF Convention, punishing such fraudulent conducts.[9]

Italy and Romania, on the contrary, have not completely adapted their legislation;[10] yet, as far as Italy is concerned, criminal behaviours included in this phenomenological context are covered by other criminal provisions.

With regard to the preparatory activities aiming at the commission of a fraud against the Community, the PIF Convention itself has established that the Member States adopt the dispositions necessary to punish them. Most States, however, have not formulated an independent crime, as they consider adequate the general rules of criminal law concerning participation and instigation[11].

Rules having a general character in the matter of participation in the crime are applicable to the offences concerning identity-related fraud.

5. Conclusions and *de jure condendo* perspective

5.1. At empiric level

Phenomena - cybercrime

- Illegal access (hacking and cracking)
- Data and system interference (D.o.S., malware, malicious code and, in general, crimeware/bot, Trojan Horse e spyware: damaging, deletion, deterioration, alteration or suppression of computer data or serious hindering right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data)
- Computer system-related fraud (input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system)
- Identity theft (theft of personal data)
- Identity related fraud and phishing (identity theft, identity

Phenomena – criminal offences committed using new technologies

- Fraud within EU or against the financial interests of the EU
- Other common frauds
- Money laundering
- Investment fraud
- Business fraud
- Theft of personal data
- Unlawful (or without right) processing of data
- Forgery (documentation-related forgery)

[9] See COMMISSION STAFF WORKING PAPER - Annex to the - SECOND REPORT FROM THE COMMISSION - Implementation of the Convention on the protection of the European Communities' financial interests and its protocols - Article 10 of the Convention {COM(2008) 77 final}.
[10] Ibidem
[11] Ibidem.

abuse, identity fraud and online frauds)
- Data interception (sniffing)
- Computer-related forgery (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)
- Unlawful Hosting
- Unlawful web pages or sites (pharming)

5.2. At criminal law level

At the level of a systematic distinction among the above mentioned different offenses, the present international picture is marked by the presence of the so-called "traditional" ("propri") computer-related crimes, for which the typical mean of commission of the offence or the passive objects of the illicit conduct have a "technological nature", on the basis of their specific definition (i.e. illegal access, computer-related fraud, data and system interference, data interception), and of the so-called common computer-related crimes, i.e. traditional crimes (such as fraud within EU, other frauds, money laundering) that more and more often are committed through means, tools and computer systems; they are included in the field subject to analysis and particular attention, above all for the common need about investigations and evidence collection and storage, although such "technological" forms are not even essential elements of the crime.

At an over-national normative level, the growing attention of the European Union to cybercrime is manifest in the adoption of the framework decisions and in the communications concerning the information society fostering the exchange of information and the cooperation among States. However, at present the most important international instrument against cybercrime is the Convention on Cybercrime of the Council of Europe, ratified by 23 States, among which most European States[12].

At national level we observe a positive trend towards the harmonization of dispositions on criminal matters, mainly after the ratification of the above mentioned Convention, providing a "strong" core of "common" rules. In particular, in the States considered in this research there exists legal instruments of protection of the confidentiality, integrity and availability of computer data and systems and against criminal offences such as computer-related forgery and computer-related fraud, as well as at the level of corporate liability.

Yet, among the single regulation there still exists a large number of discordant elements, both at the level of substantive criminal law, where we observe, for example, the lack of specific dispositions in the matter of identity-related fraud and of identity theft (due to the possible enforcement of different rules in the States) and at the level of procedural criminal law.

To this purpose, with regard not only to traditional computer-related crime ("in senso proprio"), but also to all the so-called non-traditional cyber crimes ("in senso improprio"), the dispositions of the Convention on

[12] PICOTTI, *La legge di ratifica della Convenzione Cybercrime. Aspetti di diritto penale sostanziale*, in *Dir. pen. proc*., 2008, 700 ff..

Cybercrime can represent a sound starting point, as they outline and, partially, they already regulate new and adequate provisions.

Let's consider particularly the new provisions in the matter of real-time collection of computer data and interception of content data, that in urgent circumstances provide the possibility to "make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication" (: article 25 CoC.

In a future perspective, the Treaty of Lisbon can already fill a gap, as it contains the juridical basis necessary to ground the competence of the Union in criminal-law matters in such areas of crime that present the double character of seriousness and of over-nationality (such as cybercrime)[13].

Contacts

Dr. Roberto Flor

Faculty of Law, University of Verona
Via Montanari, 9 - 37122 Verona – Italy

http://www.robertoflor.blogspot.com

flor_roberto@yahoo.it
roberto.flor@univr.it

[13] See FLOR, *Criminal Law from the Perspective of the Reform of the European Treaties*, in *Eucrim*, 1-2, 2008, 19.