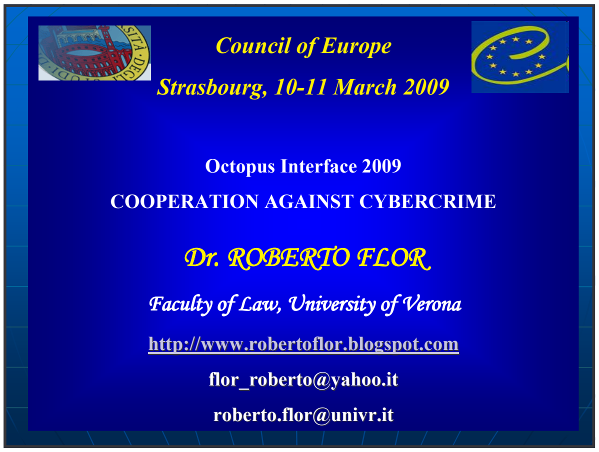


Council of Europe

Strasbourg, 10-11 March 2009

Octopus Interface 2009

COOPERATION AGAINST CYBERCRIME

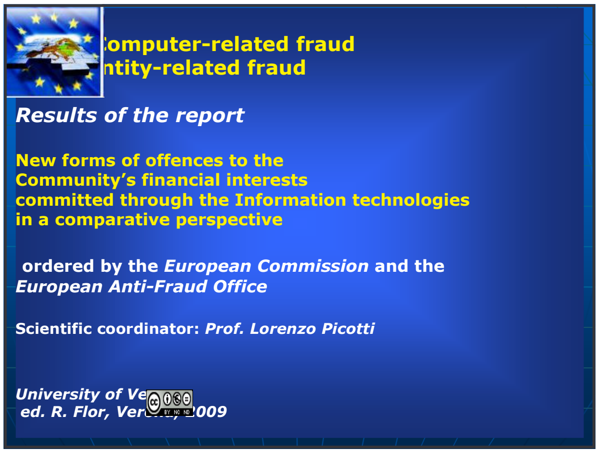
Dr. ROBERTO FLOR

Faculty of Law, University of Verona

http://www.robertoflor.blogspot.com

flor_roberto@yahoo.it

roberto.flor@univr.it



omputer-related fraud
ntity-related fraud

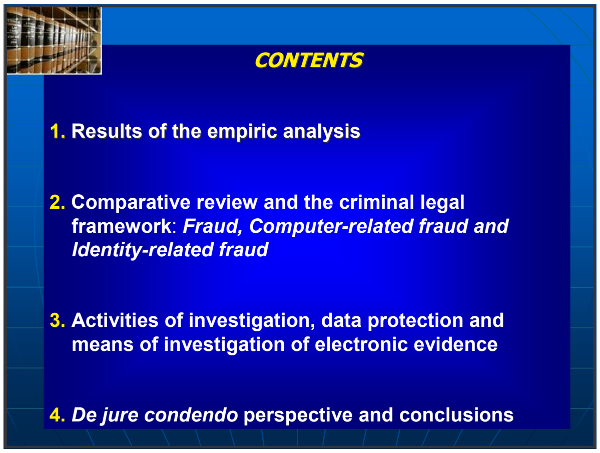
Results of the report

New forms of offences to the
Community's financial interests
committed through the Information technologies
in a comparative perspective

ordered by the *European Commission* and the
European Anti-Fraud Office

Scientific coordinator: *Prof. Lorenzo Picotti*

University of Ve
ed. R. Flor, Ver 2009



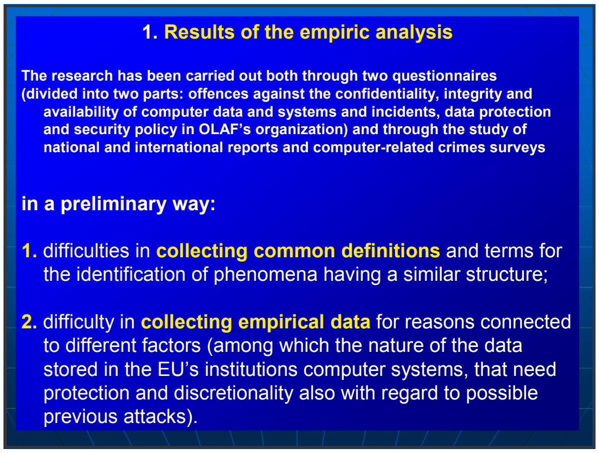
CONTENTS

1. Results of the empiric analysis

2. Comparative review and the criminal legal framework: ***Fraud, Computer-related fraud and Identity-related fraud***

3. Activities of investigation, data protection and means of investigation of electronic evidence

4. *De jure condendo* perspective and conclusions



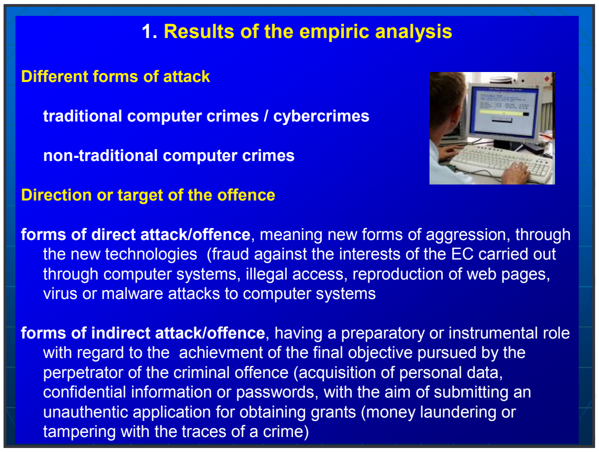
1. Results of the empiric analysis

The research has been carried out both through two questionnaires (divided into two parts: offences against the confidentiality, integrity and availability of computer data and systems and incidents, data protection and security policy in OLAF's organization) and through the study of national and international reports and computer-related crimes surveys

in a preliminary way:

1. difficulties in **collecting common definitions** and terms for the identification of phenomena having a similar structure;

2. 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).



1. Results of the empiric analysis

Different forms of attack

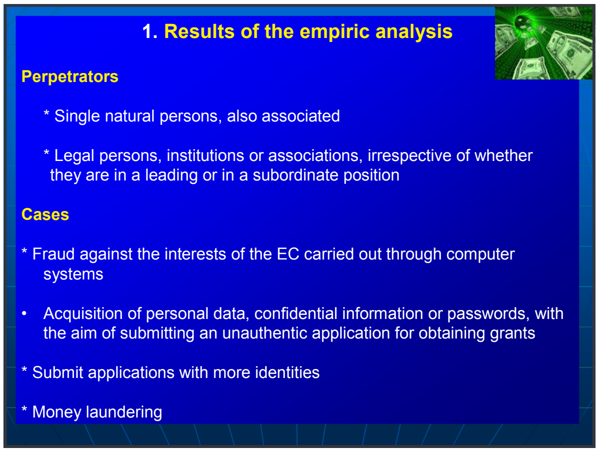
traditional computer crimes / cybercrimes

non-traditional computer crimes

Direction or target of the offence

forms of direct attack/offence, meaning new forms of aggression, through the new technologies (fraud against the interests of the EC carried out through computer systems, illegal access, reproduction of web pages, virus or malware attacks to computer systems

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 (acquisition of personal data, confidential information or passwords, with the aim of submitting an unauthentic application for obtaining grants (money laundering or tampering with the traces of a crime)



1. Results of the empiric analysis

Perpetrators

* Single natural persons, also associated

* Legal persons, institutions or associations, irrespective of whether they are in a leading or in a subordinate position

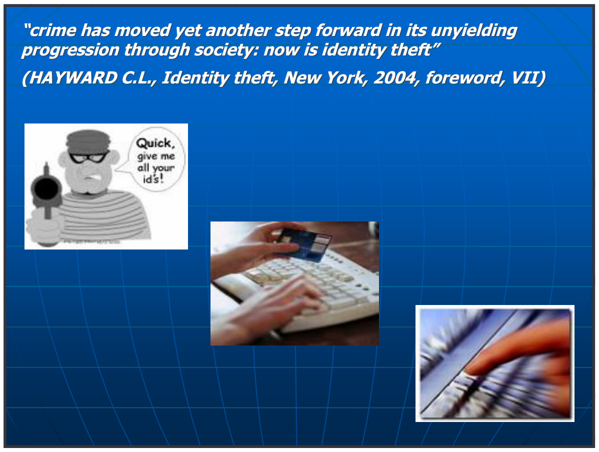
Cases

* Fraud against the interests of the EC carried out through computer systems

- Acquisition of personal data, confidential information or passwords, with the aim of submitting an unauthentic application for obtaining grants

* Submit applications with more identities

* Money laundering



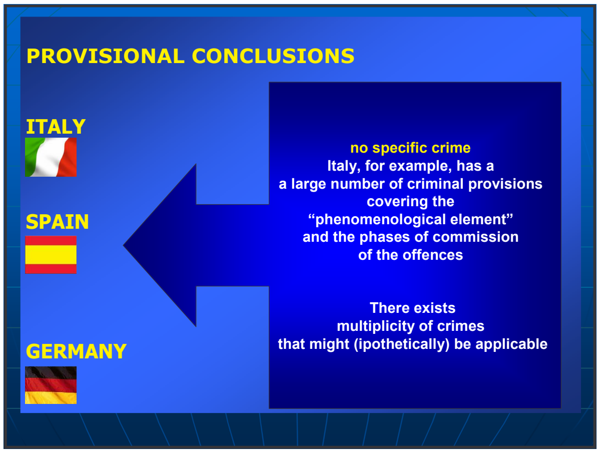
"crime has moved yet another step forward in its unyielding progression through society: now is identity theft"

(HAYWARD C.L., Identity theft, New York, 2004, foreword, VII)

2. Comparative review and the criminal legal framework

ITALY
GERMANY
SPAIN
FRANCE
ROMANIA

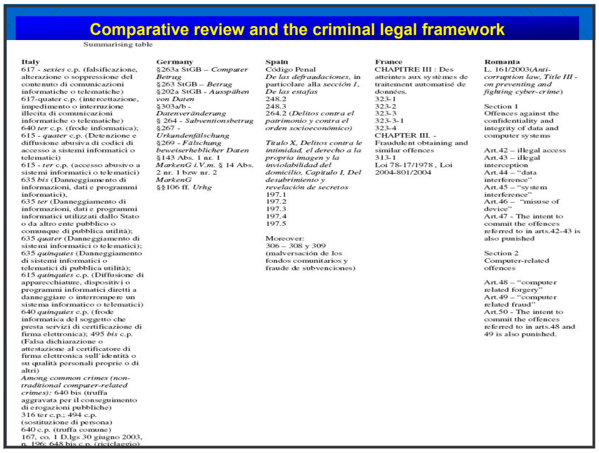
no specific crime for phenomena such as identity-related fraud; however, there exists a large number of criminal provisions covering the "phenomenological elements" and the phases of commission of the offences



PROVISIONAL CONCLUSIONS

no specific crime Italy, for example, has a large number of criminal provisions covering the "phenomenological element" and the phases of commission of the offences

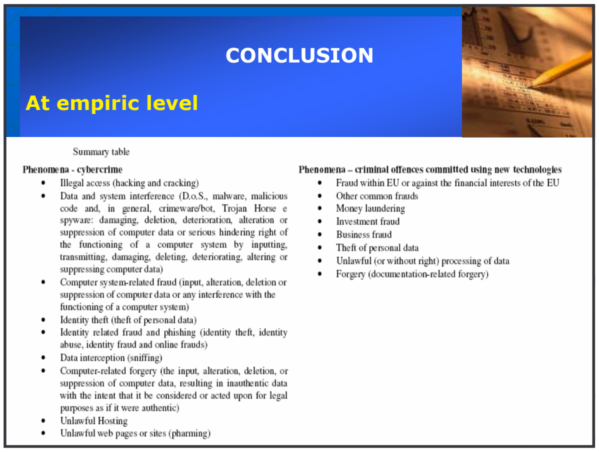
There exists multiplicity of crimes that might (ipothetically) be applicable



Comparative review and the criminal legal framework

Summarising table

Italy	Germany	Spain	France	Romania
617 - *sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche) 617-quater c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche) 640 *ter* c.p. (frode informatica); 615 - *quater* c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici) 615 - *ter* c.p. (accesso abusivo a sistemi informatici o telematici) 635 *bis* (Danneggiamento di informazioni, dati e programmi informatici), 635 *ter* (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità); 635 *quater* (Danneggiamento di sistemi informatici o telematici); 635 *quinquies* (Danneggiamento di sistemi informatici o telematici di pubblica utilità); 615 *quinquies* c.p. (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematici) 640 *quinquies* c.p. (frode informatica del soggetto che presta servizi di certificazione di firma elettronica); 495 *bis* c.p. (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri) *Among common crimes (non-traditional computer-related crimes):* 640 bis (truffa aggravata per il conseguimento di erogazioni pubbliche) 316 ter c.p.; 494 c.p. (sostituzione di persona) 640 c.p. (truffa comune) 167, co. 1 D.lgs 30 giugno 2003, n. 196; 648 bis c.p. (riciclaggio)	§263a StGB – *Computer Betrug* §263 StGB – *Betrug* §202a StGB - *Ausspähen von Daten* §303a/b - *Datenveränderung* § 264 - *Subventionsbetrug* §267 - *Urkundenfälschung* §269 - *Fälschung beweiserheblicher Daten* §143 Abs. 1 nr. 1 *MarkenG i.V.m.* § 14 Abs. 2 nr. 1 bzw nr. 2 *MarkenG* §§106 ff. *Urhg*	Código Penal *De las defraudaciones*, in particolare alla *sección 1*, *De las estafas* 248.2 248.3 264.2 (*Delitos contra el patrimonio y contra el orden socioeconómico)* *Titulo X, Delitos contra le intimidad, el derecho a la propria imagen y la inviolabilidad del domicilio, Capìtulo I, Del desubrimiento y revelación de secretos* 197.1 197.2 197.3 197.4 197.5 Moreover: 306 – 308 y 309 (malversación de los fondos comunitarios y fraude de subvenciones)	CHAPITRE III : Des atteintes aux systèmes de traitement automatisé de données. 323-1 323-2 323-3 323-3-1 323-4 CHAPTER III. - Fraudulent obtaining and similar offences 313-1 Loi 78-17/1978 , Loi 2004-801/2004	L. 161/2003(*Anti-corruption law, Title III - on preventing and fighting cyber-crime*) Section 1 Offences against the confidentiality and integrity of data and computer systems Art.42 – illegal access Art.43 – illegal interception Art.44 – "data interference" Art.45 – "system interference" Art.46 – "misuse of device" Art.47 - The intent to commit the offences referred to in arts.42-43 is also punished Section 2 Computer-related offences Art.48 – "computer related forgery" Art.49 – "computer related fraud" Art.50 - The intent to commit the offences referred to in arts.48 and 49 is also punished.



CONCLUSION

At empiric level

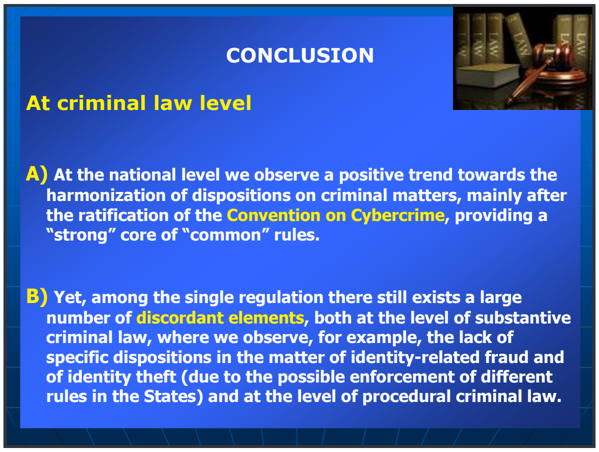
Summary table

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 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)

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)

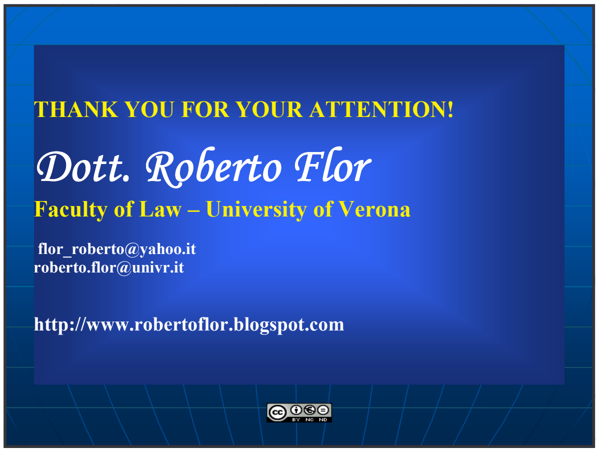


CONCLUSION

At criminal law level

A) At the national level we observe a positive trend towards the harmonization of dispositions on criminal matters, mainly after the ratification of the Convention on Cybercrime, providing a "strong" core of "common" rules.

B) 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.



THANK YOU FOR YOUR ATTENTION!

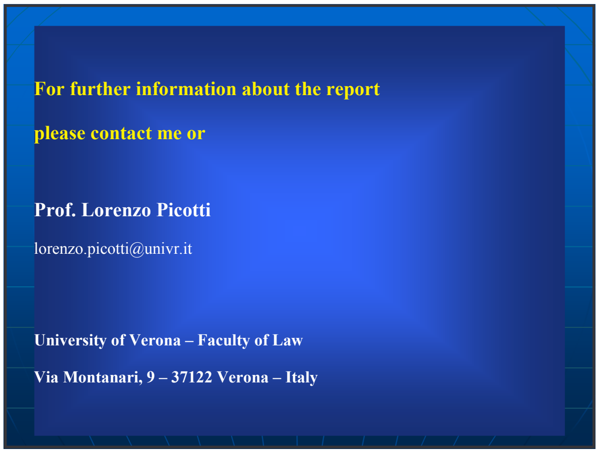
Dott. Roberto Flor

Faculty of Law – University of Verona

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

http://www.robertoflor.blogspot.com

BY NC ND



For further information about the report

please contact me or

Prof. Lorenzo Picotti

lorenzo.picotti@univr.it

University of Verona – Faculty of Law

Via Montanari, 9 – 37122 Verona – Italy