ISSN 2177-6784

# Sistema Penal & Violência

**Revista Eletrônica da Faculdade de Direito**
Programa de Pós-Graduação em Ciências Criminais
Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS

**Porto Alegre • Volume 2 – Número 1 – p. 1-17 – janeiro/junho 2010**

Editor
Rodrigo Ghiringhelli de Azevedo

Organização de
Paulo Vinícius Sporleder de Souza
Fabio D'Ávila
Nereu Giacomolli

# COUNCIL OF EUROPE CONVENTION ON CYBER CRIME AND ITS RATIFICATION IN THE ITALIAN LEGAL SYSTEM

*Marco Grotto*
University of Trento.

Abstract

The aim of this article is to describe Council of Europe recommendations, codified in the Budapest Convention, and to compare the Convention text with the Italian legislation. The focus is only on substantial criminal law, while issues of procedural criminal law institutions will be bracketed.
**Keywords:** Council of Europe Convention; cyber crime; Italian legal system.

Resumo

***Convenção do Conselho da Europa sobre crime cibernético e sua ratificação no sistema jurídico italiano***

O objetivo deste artigo é descrever recomendações do Conselho da Europa, codificadas na Convenção de Budapeste, e comparar o texto da Convenção com a legislação italiana. Embora o foco seja apenas sobre o direito penal substancial, questões institucionais de direito processual penal serão consideradas em conjunto.
**Palavras-chave:** Conselho da Europa; crime cibernético; sistema jurídico italiano.

## 1 INTRODUCTION

Modern society depends from new technologies for an increasing number of aspects. It would be difficult to image our life without computers and especially the global network called Internet. We use computer system for several activities including simple ones (i.e. shopping with credit cards) as well as complex ones (i.e. financial transactions and air traffic control).

This paper builds on the following assumption: the information technology is neither 'good' nor 'bad'. It is only an instrument. The principle of 'technological neutrality' is part of the EU legal system as attested, for instance, by the Directive 1999/93/EC of the European Parliament and of the Council issued on 13 December 1999 and dealing with the creation of a Community framework for electronic signatures. This Directive focuses on documental forgery and introduces the principle that 'member States may make the use of electronic signatures in the public sector subject to possible additional requirements' but 'such requirements shall be objective, transparent, proportionate and *non-discriminatory*' (see Clarizia 2006). Considering that the global market has no chance to develop without long distance communication systems, the IT can be considered a great opportunity for social development.

Nevertheless, it is also a great opportunity from criminal activities (i.e. *phishing*; Perri 2008; Flor 2007). As the world becomes increasingly dependent on global computer networks, the vulnerability of users – either are they private, corporate or government – increases since the probability of criminal intrusion and misuse.

Fears about Internet 'darker' criminal dimension have characterized the last decade of its popular use. As Yar (2006: 3) has noted, threats to economic performance and stability, ranging from vandalism to 'e-fraud' and 'piracy', are strongly increasing; governments talk of 'cyber warfare' and 'cyber terror'; parents fear for their children's online safety because of perverts and paedophiles stalking the Internet's 'chat rooms' looking for victims. Hardly a computer user exists who has not been subjected to attack by 'viruses' and other forms of malicious software; thedefenders of democratic rights and freedoms see a threat from the State itself, convinced that the Internet furnishes a tool for surveillance and control of citizens.

A major problem for the study of the cybercrime is the absence of a consistent current definition (Yar 2006: 9). The term has no specific referent in law, yet it is often used in political, criminal justice, media, public and academic discussion (Wall 2001: 2). For example, Thomas e Loader (2000: 3) conceptualize cybercrime as those computer mediated activities which are either illegal or consider illicit by certain parties and which can be conducted through global electronic networks. As Picotti (2004: 28) says, a distinction must be made between 'computer crimes' and 'cyber crimes'. When in 1993 Italy adopted the first law against computer related criminality (no. 547), the assumption underpinning Italian law was to punish behaviours made against or made through PCs. Nevertheless, PCs were thought as 'single' computer, not connected to others. Later, the real problem became that of protecting PCs from logical and remote access attacks and not only from physical or local attacks. From the 1960s to the 1990s computers (and Internet) made their way into companies and Public Administrations; from the 1990s to nowadays computers made their way into everyone's life (Yar 2006: 7, for instance, reminds that the first commercial browser, Netscape, was launched in 1994; for a chronological table see Council-of-Europe 2005: 84).

Therefore, whereas computer attacks made against or through 'PCs' are called 'computer crimes', computer attacks made against or through 'computer systems', which are computers connected to the global network, are called 'cyber crimes'.

Over the past few years computer networks have changed the world into a global information society in which there are virtually no frontiers, neither for their lawful use, such as educational, scientific or commercial purposes, nor for criminal misuse, such as the launch of virus attacks or the distribution of paedophile movies. There is a revolution going on in criminal activities. It creates major problems for law enforcement in almost every part of the world. The revolution lies in the ways that networked computers and other technologies permit crimes to be committed remotely, via the internet and wireless communications. A criminal no longer needs to be at the actual scene of the crime. The possibility of an international element has been added to almost any crime, which means that cumbersome mechanism for international cooperation can slow or derail many more investigations than ever before. On this context the illegal computer mediated activities can be divided into 'computer-assisted crimes' – those crimes that pre-date Internet, but which take on a new life in cyberspace; i.e. fraud, theft, money laundering, sexual harassment, hate speech, pornography – and 'computer-focused crime' – those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it; i.e. hacking, viral attacks, website defacement (Furnell 2002: 22; Lilley 2002: 24).

Against this scenario of 'global network' and 'global information', criminal activities also overcome the State borders. Computer related crimes are international in nature. For that reason an effective law reactions against cyber crimes is not thinkable without interstate cooperation. Secure networks depend to a large

extent on Governments' abilities to develop coordinated responses to criminal activities targeting or misusing computer systems. For instance, a computer related fraud made by an Italian using a German server and damaging an English costumer can not be persecuted only by Italian or German or English authorities. Instead different police authorities have to cooperate together. When investigating computer crimes, national borders become a real obstacle for law enforcement: while the internet may be borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. As a result, national authorities become increasingly dependent on cooperation with foreign counterparts. And for do that, different members States shall adopt a similar legislation: only if the same behaviour is a criminal offence the whole Europe, the police department can understand each other and efficiently cooperate. Different legal systems and disparities in the law often present major obstacles in mutual assistance. The failure of a country to criminalise computer related offences is one such obstacles. When one country's law criminalises certain activities on computers and another country's law does not, cooperation in solving a crime and prosecuting the perpetrator may be impossible. That is, when a criminal weaves his communications through several countries before reaching his indented victims, inadequate law in just of one of those countries can, in effect, shield that criminal from law enforcement around the world.

Another problem is represented by the difference between 'high tech crimes' on the one hand and 'old fashioned law enforcement tools' on the other hand (Csonka 2004: 8). Harmonization of the definitions of criminal behaviours is essential, but it is not enough. Often, to succeed in identifying such criminals, investigators must quickly follow a trail of communications from one point, such as a victim computer in a computer hacking case, to the computer where the criminal is located, often by tracing the communication through the net. To trace this communication, law enforcement authorities often must rely on historical transactional records, that is stored records of the source and destination of a communications. To succeed, law enforcement officers must have the authority to compel Internet service providers or telecom operators to access or preserve log files, electronic mail records and other critical evidence, and to do so quickly, before critical information is altered or deleted (as far as concerns this problem, on 15 March 2006, the European Parliament and of the Council issued Directive no. 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, which also amends Directive no. 2002/58/EC; for a comment: Stracuzzi 2008). If investigating authorities cannot quickly obtain this information from providers and use it to match a crime with a source computer, the investigation may be frustrated.

Many of such procedural hurdles and problems in international cooperation were considered by the Council of Europe when it issued its documents on computer crime. The idea is that certain law enforcement powers, created for and usually applied in traditional investigations, must be adapted to the specific nature of investigations in computer systems, both domestically and for rendering mutual assistance. Most of Council of Europe recommendations have now been incorporated into the Convention on cyber crime, which requires from contracting States a full compliance.

Substantially, international cooperation have to be developed in three levels (Csonka 2004: 6). First, national police and judicial authorities must have the legal tools and practices in place to provide each other prompt mutual assistance in investigating and prosecuting computer related crimes. Second, governments must enable direct collaboration between those government agencies entrusted with advancing the growth and security of e-commerce and those charged with protecting the safety of the public. Finally, the private sector plays a critical role in assuring security and confidence in shared networks and governments must work closely with industry at a variety of levels to respond to the problems associated with cyber crime.

The aim of this article is to describe Council of Europe recommendations, codified in the Budapest Convention, and to compare the Convention text with the Italian legislation. The focus is only on substantial criminal law, while issues of procedural criminal law institutions will be bracketed.

## 2 THE 1989 COUNCIL OF EUROPE RECOMMENDATION NO. R (89) 9

The Council of Europe made a first attempt to harmonise substantive computer crime law in 1989 by issuing guidelines to national law makers in its member States (see Recommendation no. R (89) 9 on computer related crime and final report of the European Committee on Crime Problems).

Specifically, the Council recommended that a minimum list of computer specific offences would be considered for ensuring a uniform European criminal policy in this area.

This list included the definition of eight offences (computer related fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of a topography) and was supplemented by an optional list which contained four additional offences (alteration of computer data or computer programs, computer espionage, unauthorised use of a computer, unauthorised use of a protected computer program). Italy complied to EU Recommendation with the law no. 547/1993 (see, in particular, Pecorella 2006; Picotti 2004; Picotti 2000 and Picotti 1996). This law deeply modified the Penal Code and Procedural Criminal Code. Most of the rules contained in law no. 547 have not been revised by the later law no. 48/2008, through which the Italian Parliament ratified and gave execution to the Budapest cyber crime Convention.

In 1997, a report on the implementation of EU Recommendation guidelines concluded that no sufficient harmonization was achieved. The observers noted that significant discrepancies remained in member States' legislation and that a binding legal instrument, a treaty, would be necessary to enable effective international cooperation. In the absence of harmonised computer crime laws, investigations involving several nations are indeed bound to fail, for example due to lack of dual criminality (i.e. the nations concerned do not have similar l aws banning the conduct), a principle that governments must observe to obtain cooperation, whether mutual assistance or extradition, from other nations (Garcia 2004; Picotti 2005).

## 3 THE COUNCIL OF EUROPE'S CONVENTION ON CYBER CRIME. AN INTRODUCTION

By the decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. The EU Convention on cyber crime is the result of four years of intensive work by an expert committee set up in 1997, the 'Committee of Experts on Crime and Cyberspace' (also called 'Committee PCCY'), which was entrusted by the Committee of Ministers to follow up on previous Council of Europe recommendations on computer crime and criminal procedure problems linked with information technology. The Committee was given the particular task to prepare a legally binding instrument, a treaty (Guernelli 2008). The Committee completed its work at the end of the year 2000 and worked in close coordination with the G-8 and other international bodies on the draft Convention on cyber crime.

The European Committee on Crime Problems approved the final draft of the Convention in June 2001. The Committee of Ministers adopted the Convention on cyber crime on 8 November 2001 in Budapest, in the occasion of an international conference. Thirty States signed immediately the Convention, among which twenty-six Council of Europe member States and four non member States which had participated to the drafting process (United States, Canada, Japan and South Africa). Evidently, the US participation at the Convention works had an important role because, as Yar 2006 and Salvadori 2008 note, the US introduced one of the

earliest national laws specifically oriented to computer crime in the form of the Computer Fraud and Abuse Act – CFAA of 1984.

As publicized in the Convention website, the Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

Several of member States which signed the treaty experienced difficulty or delay of adapting domestic law to the requirements of the Conventions. Italy is one of these States. Indeed, the domestic law which ratified the Convention was only approved on March 2008 (law no. 48/2008).

The treaty signed in Budapest on 23 November 2001 has received strong support from lawmakers and practitioners throughout Europe and beyond, but has also been criticised on various grounds by a numbers of associations, particularly those active in the protection of freedom of expression (Csonka 2004). That demonstrates that one of most difficult things in fighting cyber crime is to balance the prevention of crimes with individual rights, like privacy, freedom of speech and similar.

The Convention is a very important instrument of cooperation. Indeed it has been signed by several Council of Europe member States, but also by Canada, Japan, United States of America and South Africa.

The Convention on cyber crime has three aims (Csonka 2004: 13). The first aims is to lay down common definitions of certain criminal offences, which is very relevant to harmonize legislation at national level. Following EU customary convention, article no. 1 contains the definitions of "computer system", "computer data", "service provider" and "traffic data". However, the Italian law of cyber crime Convention did not introduce the EU definition in the domestic law system (Guernelli 2008: 755). In doing this the Convention aims at harmonizing domestic legal system by providing a common definition against existing different meanings across EU members' legal systems. The first part of the Convention concerns the introduction of harmonized criminal offences in the legislation of future contracting States, which could eliminate problems of dual criminality.

The second aim of the Convention is to define common types of investigative powers better suited to the information technology environment, thus enabling criminal procedures to be brought into line between countries. Such powers will be available for the investigation and prosecution of offences defined under the Convention, as well as of other offences committed by means of a computer system or whose evidence is in electronic form.

Finally, the Convention aims at determining both traditional and new types of international cooperation, thus enabling cooperating countries to rapidly implement the arrangements for investigation and prosecution advocated by the Convention, by using a network of permanent contacts.

As far as concerns the structure, the Convention contains four chapters: (I) Use of terms; (II) Measures to be taken at domestic level for substantive law and procedural law; (III) International cooperation; (IV) Final clauses. As already mentioned, this article solely focuses on sections I and II.

Chapter I (substantive law issues) covers both criminalization provisions and other connected provisions in the area of computer or computer-related crime. It first defines nine offences, grouped in 4 different categories, then deals with ancillary liability and sanctions. The Convention identifies the following offences: 'illegal

access', 'illegal interception', 'data interference', 'system interference', 'misuse of devices', 'computer-related forgery', 'computer related fraud', 'offences related to child pornography' and 'offences related to copyright and neighboring rights'. These offences, some of which are already the subject of the 1989 recommendations on computer-related crime, fail into four categories: i) offences against the confidentiality, integrity and availability of data or computer systems; ii) computer-related offences; iii) content-related offences; iv) offences involving the infringement of intellectual property and related rights. Offences in the first category all concern offences targeting computerized information, systems or data. Their nature is closely linked to the computing environment in which they take place. Although some of these offences may have an equivalent in the 'ordinary world' (for instance, illegal access or "hacking" may be comparable to home violation), making them offences in their own right is based on a clear political consideration according to which it is necessary to specifically protect computer networks and the data they contain (Grotto 2006). However, in order to be considered as an offence, these infringements must always be committed intentionally and unlawfully, "without right". There are therefore acts which, if duly authorized and executed by thestate authorities (law enforcement, intelligence or judicial) or accepted as lawful commercialpractices, will not be considered as a criminal offence under the Convention.

Chapter II (procedural law issues) determines first the common conditions and safeguardsapplicable to all procedural powers. Nevertheless, this chapter goes beyond the offences defined in the Convention in that its scope applies to any offence committed by means of a computer systemor to the electronic evidence. Chapter II then sets out the following procedural powers: expeditedpreservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data. The Chapter concludes with the jurisdiction provisions. Chapter III contains the provisions concerning traditional and computer crime related

mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between contracting countries – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer related crimes apply to both situations and cover, subject to extra conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of trans border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the contracting States.

Finally, Chapter IV contains the final clauses, which – with certain exceptions – repeat the standard provisions in Council of Europe treaties (Csonka 2004). As far as concerns computer attacks, the Council has recently issued the important Framework Decision no. 2005/222/JHA (24 February 2005) dealing with attacks against information systems. This Framework Decision also invites each Member State to take the necessary measures to punish as a criminal offence (i) the intentional access without right to the whole or any part of an information system (article no. 2, 'Illegal access to information systems'), (ii) the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data (article no. 3, 'Illegal system interference'), (iii) the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system (article no. 4, 'Illegal data interference'). Still, the EU Framework Decision forces to punish instigation, aiding and attempt. Concerning penalties, as it is usual for EU Acts, the EU Framework Decision provides that offences have to be punished by 'effective', 'proportional' and 'dissuasive' penalties. The Framework, however, adds something new to the 'EU criminal

law system' by specifying that, for illegal system and data interference, each member State shall introduce 'criminal penalties' of a maximum of at least between one and three years of imprisonment. Liability of legal persons is also introduced.

## 4 THE IMPLEMENTATION OF CONVENTION OF BUDAPEST IN THE DOMESTIC LEGISLATION

### 4.1 Illegal access

By criminalising the mere illegal access (Convention, article no. 2), i.e. "hacking", "cracking" or "computer trespass" (on this topic see Salvadori 2008), governments wanted to send a clear signal that this conduct is illegal in itself and will be prosecuted, particularly as it is considered a kind of base-lime offence: such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without right or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery (Csonka 2004: 15). The United States of America declares that under their law the offenses set forth in article no. 2 ('Illegal access') includes an additional requirement of intent to obtain computer data. Many national legislations already contain provisions on "hacking" offences. Italy, for instance, is one of these countries. The article no. 615-ter of the Penal Code[1], introduced by the law no. 547/1993 (adopted to comply with the 1989 EU Recommendation) specifically criminalizes the illegal access to a computer system protected by security measures (Flor 2008). The judicial courts often compare illegal access to a computer system with the illegal access to a private property (article no. 614, Penal Code[2]). Article no. 614 of the Penal Code relates to an offence to the 'private domicile' ("domicilio privato"). Article no. 615-ter of the Penal Code relates to an offence to the 'informatics domicile' ("domicilio informatico").

Picotti (1996), however, criticizes the courts' way of thinking preferring to talk of "informatics privacy" (in Italian: "riservatezza informatica") or, using the Convention's words, the 'confidentially of computer data and systems'.

In the Italian system, the 'confidentially of computer systems' is also protected by article no. 615-quarter[3] of the Penal Code, which provides a sanction for those who illegally obtain passwords or other codes to have access to a computer system. This rule is similar to the one contained in article no. 6, part 1.a.ii. of the Convention, which is referred to the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed. Article no. 615-ter and 615-quarter of the Italian Penal Code were introduced by law no. 547/1993 and have not been modified by the law no. 48/2008 of the ratification of cyber crime Convention.

### 4.2 Illegal interception

The provision on illegal interception (Convention, article no. 3) aims to protect the right of privacy of data communications (Csonka 2004: 16). The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons and applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer. The offence applies to 'non public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Alternatively data may be kept secret for commercial purposes until the service is paid. Therefore, the term 'non-public' does not *per se* excludes communications via public networks.

In Italy, the protection of computer transmissions is quite complex. There is a general rule (Penal Code, article no. 616[4]) which provides a sanction for those who read or destroy a message addressed to another person. This article, like EU Convention rules, makes a distinction between 'open mail' (in Italian, "corrispondenza") and 'close mail'. The last sentence of article no. 616 specifies that the word 'mail' is referred to both paper and digital one. This rule and the ones coming immediately afterwards (from article no. 617 to article no. 623-bis) can be read as the implementation of the constitutional principle of 'mail secrecy' (see the Italian Constitution, article no. 15). This article is also relevant for the judicial courts when they have to solve problems concerning employees' e-mail checking by employers. In the majority of the pronounce sentences, the courts conclude that the firm e-mail is a job instrument, which, in specific cases, can also be checked by the employer (Giudice per le Indagini Preliminari di Milano, 10.5.2002; Tribunale di Torino, 20.6.2006-15.9.2006, n. 143; Corte Europea dei Diritti dell'Uomo, 3.7.2007; Corte di Cassazione, sezione V, 11.12.2007-19.12.2007, n. 47096). On this topic, the Italian Authority for personal data protection on 1 March 2007 adopted 'Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context' in which it specified that, in general, the correspondence is secret and inviolable. Nevertheless, firms may adopt an internal protocol in which they explicitly indicate that the e-mail is only a job instrument and that the employer has the right to know workers' personal password, to check his/her email when it is necessary for the industrial activity even when the worker is absent from work for illness or vacation reasons.

Focussing on the issue of illegal interception, the Italian Code provides six different criminal offences. Three of those were introduced by the Act no. 98/1974, which represents the first Italian law concerning privacy protection, intended as 'right to be alone' (later, in EU acts, the privacy right was no longer meant as the 'right to be alone' but as the right of managing personal data). Specifically, article no. 617, 617-bis and 617-ter refer to telephone or telegraphic interceptions. Later, in 1993, the legislator extended this three criminal offences to computer data transmission, introducing articles no. 617-quater, 617-quinquies and 617-sexies (Plantamura 2006; Cajani 2006).

It is worth noting, however, that the jurisprudence on this topic is scarce (Cajani 2006). Only rare judgements were pronounced drawing on articles from no. 617-quarter to 617-sexies (e.g.: Corte di Cassazione, sezione V, 1.2.2006, n. 4011).

### 4.3 Data and system interference

The provision on data interference (Convention, article no. 4) aims at providing computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional damage (Csonka 2004: 16). Conduct constituting the offence, such as damaging, deteriorating or deleting computer data, involve a negative alteration of the integrity or of information content of data and programmes. Input of data, such as malicious codes and viruses like Trojan horses, also fall within the scope of the provisions on data interference.

The provision on system interference (Convention, article no. 5) aims at criminalising acts of computer sabotage. The offence covers the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The text is formulated in a neutral way so that all kinds of system functions can be protected by it. The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data. As opposed to data interference, the hindering of computer systems must be "serious" in order to give rise to criminal sanction. For instance, it can be considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other

systems (i.e. by means of programs that generate "denial of service" – DoS attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system). In the Italian legal system, the issue of data and system interference has been dealt with in two steps. First, in 1993, the legislator introduced two new articles. On the one hand, the legislator introduced article no. 635-bis in the Penal Code. This article was put right afterwards article no. 635, which protects private property from damages, thereby suggesting that damaging to data and computer is no different from damaging to private property. On the other hand, the legislator introduced article no. 420 which concerns public order. Article no. 635-bis can be considered as an implementation of the 1989 EU Recommendation. Article no. 420, instead, was drafted in response to the turmoil sparked by some separatist groups in the extreme northern part of the country. Article no. 420 provides a sanction for those who makes an attempt to public structures. In 1993, then, the rule was extended 'informatics structures of public duty'. Second, in 2008, with the Act no. 48 that implemented the cyber crime Convention, article no. 420 was abrogated and the rule of article no. 635-bis was divided into four different offences (Penal Code, article no. 635-bis[5], 635-ter[6], 635-quater[7] and 635-quinquies[8]). First, articles no. 635- bis and 635-ter only referred to computer data and computer programs damaging. As a result, these offences can be linked to article no. 4 of the Convention on cyber crime, which deals with 'data interference'. Second, article no. 635-quater and 635-quinquies referred not to data but to system damaging. These articles can therefore be linked to article no. 5 of the EU Convention.

Finally, whereas both articles no. 635-bis and no. 635-quarter are related to the damaging of data and programs, the article no. 635-bis concerns damaging of 'private' data and programs and article 635-quarter refers to damaging of data and programs used by a public administration.

The two articles imply a different behavior. Indeed, the damaging of private data constitutes a crime only when there is real damage of data and programs. The damaging of public data, in contrast, constitutes a crime when there is an action 'directed at' damaging or destroying. Of course, the final damage can exist but it is not a necessary element for the criminal offence. The consequence is that a behaviour that is 'direct at' damaging can be qualified as a criminal offence only if it is referred to public data butit cannot be qualified as a criminal offence when it concerns the damaging of private data. The identification of the criminal offence as far as concerns articles no. 635-quater and 635-quinquies (interference in the private or a public 'system') follows the same pattern described for articles 635-bis and 635-ter.

Despite the important legislative changes introduced in 2008, many scholars think that the new situation is nonetheless confused, not least because of the distinction between 'damaging' and 'acts directed to damage' (Picotti 2008; Sarzana-di-Sant'Ippolito 2008).

### 4.4 Misuse of devices

This provision on misuse of devices (Convention, article no. 6) establishes as a separate criminal offence some specific conduct (production, distribution, sale, etc.) regarding access devices which were primarily designed or adapted for misuse (Csonka 2004: 17). Devices that are designed and used for legal purposes are not captured. It was debated at length whether the devices should be restricted to those which are designed 'exclusively' for committing offences, thereby excluding totally dual-use devices, but this sort of definition could have led to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. This offence therefore requires a particular purpose, i.e. committing any of the other offences against the confidentiality, the integrity and availability of computer systems or data, as defined in the Convention.

It is interesting to note that under US law, this offense includes a requirement according which a minimum number of items need to be possessed in order for the punishment to be applicable. The minimum number shall be the same as that provided for by applicable US federal law.

In Italy, the misuse of devices is sanctioned by article no. 615-quater[9] and 615-quinquies[10] of the Penal Code. Article no. 6 of the Budapest Convention concerns the production, sale, procurement for use, import, distribution or otherwise making available of i) a device designed or adapted primarily for the purpose of committing any of the offence established in the other articles of the Convention; 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. In the Italian legal system, article no. 615-quinquies of Penal Code reflects the Budapest Convention, article no. 6, paragraph i). Article no. 615-quater, instead, reflects the Budapest Convention, article no. 6, paragraph ii) (Catullo 2006; Luparia 2006; Rabazzi 2006). Article no. 615-quater is similar to the Convention's text, even if it was introduced in 1993 and never modified later on (even Act no. 48/2008 did not change the content of article no. 615-quater). Of course, article no. 615-quater describes an offence which can be transformed into a more serious offence when the detention of passwords is used for illegal access (article no. 2 of the Convention; article no. 615-ter of Italian Penal Code). As far as concerns article no. 615-quinquies, Act no. 48/2008 modified it in important respects. Indeed, the text introduced in 1993 qualified as a criminal offence the production or procurement, among others, of a device 'designed for' committing a cyber offence.

After 2008, the offence consists in producing or procuring, among others, devices or programs. Essentially, in contrast to the 1993 legislation, today's article no. 615-quinquies does not contain a reference to the goal for which the devices are used! In other words, today, the misuse of device does not concern the behaviour, but only the *mens rea*: the offence is based on procuring, importing, etc. devices 'with the purpose of damaging a computer system, data, programs or information'. The literature (Picotti 2008; Sarzana-di-Sant'Ippolito 2008) has strongly criticized the new wordings of article no. 615-quinquies because the distinction between a legal behaviour ('using programs') and an illegal behaviour ('using program with the purpose of damage') is based only on the actor's *mens rea* and not also on the specific characteristics of the programs used by him.

### 4.5 Computer related forgery and computer related fraud

The offences that fall within the second category of the Convention cover 'computerversions' of two offences (fraud and forgery) which are usually perpetrated in the traditional manner in the real world (Csonka 2004: 18). Nevertheless, fraud or forgery can also be perpetrated via computer networks, which consequently become the means by which the offence is committed, rather that being its target. Both fraud and forgery are basically manipulation-based conducts. The Convention's member countries thought it was necessary to introduce new separate criminal offences to punish traditional behaviours committed through the new technologies. That means that traditional offences cannot be applied to acts perpetrated through computer networks (for example, in the case of computer-aided fraud, the element of deceit is missing and in the case of computeraided forgery, the difference between an original and a copy no longer exists). Moreover, when fraud or forgery is committed through computer networks, a larger number of people is likely to suffer damages. The inclusion of fraud and forgery in the Convention attests to the fact that in many countries certain traditional legal interests are not sufficiently protected against new forms of interference and attacks. Indeed, with the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations

and other interferences with the course of data processing. The aim of provision on computer related fraud is to criminalize any illegal manipulation in the course of data processing (including input, alteration, deletion, suppression of data as well as interference with the functioning of a computer programme or system).

The aim of the provision of computer related forgery is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related in traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value and the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception (Grotto 2006).

In Italy, article no. 640-ter of the Penal Code[11] is similar to article no. 8 of the Convention (Perri 2008; Guernelli 2007). As has been the case for articles no. 615-ter and 615-quater, the domestic legislation was introduced in 1993 and it has not been modified by the law that ratified the Convention. Nevertheless, Act no. 48/2008 had a concrete impact on the topic of computer related fraud.

Two new offences were introduced. They both concern the digital signature. On the one hand, article no. 495-bis of the Penal Code[12] punishes who declares something false to the person who provides digital signature services (Flick 2008). On the other hand, article no. 640-quinquies[13] punishes forgery committed by a public certificatory, which is the person/entity who certifies the identity of the person requiring digital signature. This forgery takes place with the intent of procuring an economic benefit, for the offender or for others, or with the intent of damaging somebody else. Article no. 640-quinquies, however, is technically imperfect (Grotto 2009). It is located among offences against property, but it seems to be an offence against authenticity of information. The behaviour is a clear sort of forgery and the economic benefit/economic damage is located only on actor's *mens rea*. As far as concerns computer related forgery, this offence is contained in the article no. 491-bis of Italian Penal Code (Grotto 2006; Pica 2006).

This article extends the punishment provided for traditional documents to the informatics documents. Until 2008, the article also contained a definition of 'informatics document'.

The problem was that 'informatics document' was defined as an 'informatics support' containing data or information that are relevant for legal transactions or containing programs needed to read or modify data contained in PCs.

The most relevant problem of such a definition was that an informatics document was considered inseparable from its informatics support. In the traditional way of thinking, a document is an idea, expressed in a language that can be understand, fix on a piece of paper or other materials. In the IT world, a document is an information, a group of organized data, whose intrinsic characteristic is that it can be transmitted from one person to another without any support (Grotto 2006).

In 2008, the legislator deleted the previous definition. However, judges and scholars are not free to define the informatics document at their will, because Act no. 82/2005 contains a wide-accepted definition: informatics document is the informatics representation of acts, facts or data relevant for the legal transactions.

### 4.6 Child pornography

The third category of the offences dealt with by Convention are those concerning child pornography. In particular, the Council of Europe made this problem a top priority. As a result, the Convention identifies as offences a number of acts, including the possession and the distribution of child pornography. The provision on

child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most Convention member States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children.

As far as concerns the protection of children, the Council also adopted the framework Decision no. 2004/68/JHA (22 December 2003) on combating the sexual exploitation of children and child pornography. Here it is sentenced that each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable: i) production of child pornography; ii) distribution, dissemination or transmission of child pornography; iii) supplying or making available child pornography; iv) acquisition or possession of child pornography.

Among the other EU initiatives in force or in progress that address some of the problems which affect child sexual offences, the following Decision are worth remembering. On 29 May 2000 the Council issued the Decision no. 2000/375/JHA to combat child pornography on the internet. The Council Framework Decision no. 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States was issued on 13 June 2002 followed by the Council Framework Decision no. 2005/222/JHA on attacks against information systems on 24 February 2005. Still, there were Decision no. 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the internet and new online technologies, and Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition of judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions.

Furthermore the Council of Europe issued the Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision no. 2004/68/JHA. In Italy, child prostitution and child pornography are punished by articles from no. 600-bis to no. 600-septies of Penal Code. These offences were partly introduced in 1989 (Act no. 269) and partly in 2006 (Act no. 38) (Picotti 2007; Aterno 2006; Cadoppi 2006). It is also particularly to note that these articles punish 'virtual child pornography'[14]. That was provided by article no. 9 of the Convention. Indeed, paragraph 2 reads: «the term 'child pornography' shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct». The point is that virtual child pornography images are created with PCs and, even if contain explicit sexual acts between or with children, they do not reflect real situations. Of course, a criminal offense has to offend a public interest (what is called 'bene giuridico' in Italian). The 'real child pornography' – which supposes a real sexual act between children or between a child and an adult – has to be punished because it damages the interest to the regular development of the children sexuality. In the punishment of 'virtual child pornography', instead, there is no child to protect (the images are virtual, not real). Therefore, the norm on virtual child pornography seems to suggest that what is to be punished is a depraved way of living (maybe a sickness) and not a behaviour that offends a public interest (Picotti 2007).

The fight against child sexual exploitation also involves tour operators. In journeys brochures, for instance, they have to specify that child prostitution is strictly forbidden; if they do not specify that, they

can be fined from € 1.500 to € 6.000. Act no. 38/2006 also crated the 'Centro nazionale per il contrasto della pedopornografia sulla rete Internet'. It is a government agency that is specifically mandated to prevent child pornography, collect information and maintain a data base of suspected cases.

Finally, specific duties are contemplated for Internet service providers (Petrini 2004).

### 4.7 Infringements of copyright

The fourth category of the Convention offences involves infringement of copyright and related rights through computer networks. Such infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audiovisual and other works.

The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and improve international cooperation in this field. Each Party is obliged to criminalise infringements of copyright and related rights, arising from the agreements listed in the article (TRIPS and WIPO Copyright treaty), when such infringements have been committed by means of a computer system and on a commercial scale.

Copyright is also protected by the Directive no. 2009/24/EC of the European Parliament and of the Council issued on 23 April 2009. This Directive deals with the legal protection of computer programs and contemplates (article no. 7) that Member States shall provide, in accordance with their national legislation, appropriate remedies against i) a person committing acts of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy; ii) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy; iii) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

Recently, the European Council issued the Resolution of 16 March 2009 on the EU Customs Action Plan to combat IPR infringements for the years 2009 to 2012.

In Italy, copyright is protected by Act no. 633/1941. Criminal offences are contemplated at articles from no. 171 to 181-bis. The most important rules are article no. 171-bis, which protects computer programs and data bases (Resta 2007; Plantamura 2006), article no. 171-ter, which is referred to music or videos, and article no. 171, through which other behaviours against copyright are punished.

The copyright criminal legislation has been modified several times (see, for instance, Act no. 248/2000, Act no. 128/2004, Act no. 68/2003, Act no. 43/2005). The overlap of different rules creates a system difficult to manage.

For instance, both behaviours against informatics programs or data bases (article no. 171-bis) and behaviours against music or video works (article no. 171-ter) are punished if committed with an intent of economic benefit. However, article no. 171-ter refers to 'fine di lucro' that means that the offender aims at increasing his/her economic level. Article no. 171-bis, instead, refers to 'fine di profitto' that means that it is sufficient that the offender avoids an expense. For instance, if a person copies a PC programs with the aim of buying only one copyright licence when he needs more, he can be convicted under article no. 171-bis. Indeed, it is an expenditure saving. In contrast if a person copies a music or a movie, he/she can be punished only if he/she makes a profit from such an activity (Gallus 2008; Onorato 2003).

As far as concerns 'peer 2 peer' networks, the Italian system has three rules. First, 'downloading' material protected by copyright is considered by article no. 174-ter that provides only an administrative sanction (i.e. fine of € 154). Second, 'uploading' is a criminal offence punished under article 171-ter (imprisonment from 6 months to 3 years and fine from € 2.582 to € 15.493 Euros) if committed with profit intent ('fine di lucro'). Finally, 'uploading' is a criminal offence punished under article no. 171 (fine from € 51 to € 2.065) if committed without any specific aim.

## 5 CONCLUSIONS

The Convention on cyber crime is a useful demonstration of the importance of the interstate cooperation. An effective fight against cyber crime can only be managed through legal instruments which overcome State borders and create an intensive cooperation among police agencies.

Recently, an Additional Protocol to the Convention on cyber crime was approved (ETS no. 189). It concerns racist and xenophobic acts committed through computer systems. The protocol, which was opened for signature by the member States which have signed the Convention on 28 January 2003, entered into force on 1 March 2006. The protocol underling idea is to adopt a coordinated approach that enables an effective domestic and international response while combating racist or xenophobic propaganda.

Finally, during the last Council of Europe Conference (10 and 11 March 2009) the 'Global Project on Cyber-crime (Phase 2)' was presented. The project emphasizes that Governments must provide for the following points: i) effective criminalization of cyber offences: the legislation of different countries should be has harmonized as possible to facilitate cooperation; ii) investigative and prosecutorial procedures and institutional capacities which allow criminal justice agencies to cope with high tech crime; iii) condition facilitating direct cooperation between State institutions, as well as between State institutions and the private sector; iv) efficient mutual legal assistance regimes, allowing for direct cooperation among multiple countries.

The process of harmonization cannot be confined to a process of harmonization of civil and administrative law. Rather, harmonization will be successfully completed when a common criminal law system will be in place. This common criminal regulatory system seems to be the only appropriate response to compelling problems such as DOS attacks, data and system interference and unauthorized access.

## REFERENCES

Aterno, S. Non è punibile la mera consultazione via internet di siti per pedofili senza registrazione di dati sul disco. *Diritto dell'Internet*, 2006.

Borruso, R., G. Buonomo, G. Corasaniti, e G. D'Aietti. *Profili penali dell'informatica.* Milano: Giuffrè, 1994.

Cadoppi, A. *Commentario delle norme contro la violenza sessuale e della legge contro la pedofilia.* Padova: Cedam, 2006.

Cajani, F. I fuori onda di Striscia arrivano in Cassazione. *Diritto dell'Internet*, 2006.

Cassano, G. *Diritto delle nuove tecnologie informatiche e dell'Internet. Aspetti costituzionali, civili, commerciali, industriali, tributari, amministrativi, penali, di informatica giuridica, degli strumenti finanziari informatici, delle tecnologie applicate all'attività giudiziaria, della sicurezza informatica.* Milano: Ipsoa, 2002.

Catullo, F.G. Il caso Vierika: un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili sostanziali. *Diritto dell'Internet*, 2006.

Clarizia, R. Il Consiglio di Stato, il codice dell'amministrazione digitale e le firme elettroniche. *Diritto dell'internet*, 2006: 277.

Council of Europe. *Organised crime in Europe: the threat of cybercrime. Situation report 2004.* Strasbourg: Council of Europe Publishing, 2005.

Csonka, P. The Council fo Europe Convention on cyber-crime: a response to the challenge of th new age? In *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica*, di G. Ilarda e G. Marullo. Milano: Giuffrè, 2004.

Flick, C. Falsa identità su Internet e tutela penale della fede pubblica, degli utenti e della persona. *Il Diritto dell'informazione e dell'informatica*, 2008.

Flor, R. Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente. *Rivista italiana di diritto e procedura penale*, 2007.

Flor, R. Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto. *Diritto penale e processo*, 2008.

Forlani, E. La conservazione preventiva di dati informatici per l'accertamento di reati. *Diritto dell'Internet*, 2008.

Furnell, S. *Cybercrime: Vandalizing the information society.* London: Addison-Weslet, 2002.

Gallus, G.B. Duplicazione a scopo di profitto del software e attività professionale. *Diritto dell'Internet*, 2008.

Garcia, O.M. La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime. In *Il diritto penale dell'informatica nell'epoca di internet*, di L. Picotti. Padova: Cedam, 2004.

Grotto, M. Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491-bis c.p. *Il Diritto dell'informazione e dell'informatica*, 2006.

Grotto, M. Reati informatici e Convenzione Cybercrime. Oltre la "Truffa" e la "Frode informatica": la "Frode del certificatore". *Diritto dell'informazione e dell'informatica*, 2009.

Guernelli, M. La Convenzione sul cyber-crime e la decisione quadro relativa agli attacchi informatici:

significato e portata per il sistema penale interno. *Studium iuris*, 2007.

Guernelli, M. La legge di ratifica ed esecuzione della convenzione sul cybercrime: considerazioni sostanziali e processuali. *Rivista trimestrale di diritto penale dell'economia*, 2008.

Guernelli, M. L'uso di strumenti o sistemi informatici per la realizzazione di reati in materia patrimoniale. *Rivista trimestrale di diritto penale dell'economia*, 2007.

Lilley, P. *Hacked, attacked and abused: digital crime exposed.* London: Kogan Page, 2002.

Luparia, L. Il caso Vierika: un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali. *Diritto dell'Internet*, 2006.

Onorato, P. La tutela penale del diritto d'autore. Le fattispecie incriminatrici dopo la Legge n. 248/2000. *Cassazione penale*, 2003.

Pecorella, C. *Diritto penale dell'informatica. Ristampa con aggiornamento.* Padova: Cedam, 2006.

Perri, P. Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema

informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema. *Giurisprudenza di merito*, 2008.

Petrini, D. *La responsabilità penale per i reati via Internet.* Napoli: Jovene, 2004.

Pica, G. *Diritto penale delle tecnologie informatiche.* Torino: Utet, 1999.

Pica, G. Osservazione sui problemi del falso informatico. *Diritto dell'Internet*, 2006.

Pica, G. voce Reati informatici e telematici. *Digesto delle discipline penalistiche. Aggiornamento*, 2000.

Picotti, L. *Studi di diritto penale dell'informatica.* Padova: Cedam, 1992.

Picotti, L. Legge 23 dicembre 1993, n. 547. Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica. Art. 3. *Legislazione penale*, 1996.

Picotti, L. voce Reati informatici. *Enciclopedia giuridica Treccani*, 2000.

Picotti, L. Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati. In*Il diritto penale dell'informatica nell'epoca di Internet*, di L. Picotti. Padova: Cedam, 2004.

Picotti, L. Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale. *Diritto dell'Internet*, 2005.

Picotti, L. La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet ( l. 6 febbraio 2006, n. 38). *Studium iuris*, 2007.

Picotti, L. La ratifica della convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale. *Diritto Penale e Processo*, 2008.

Picotti, L. Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo. *Diritto dell'Internet*, 2008.

Plantamura, V. La tutela penale dei programmi per elaboratore e delle banche dati. *Rivista trimestrale di diritto penale dell'economia*, 2006.

Plantamura, V.-Manna, A. *Diritto penale e informatica.* Bari: Cacucci, 2007.

Rabazzi, C. Il reato di diffusione di virus informatici nella dottrina e nella giurisprudenza nazionale.

*Giurisprudenza di merito*, 2006.

Resta, F. Banche di dati on line. I limiti della tutela penale. *Giurisprudenza di merito*, 2007.

Salvadori, I. "Hacking", "cracking" e nuove forme di attacco ai sistemi d'informazione. Profili di diritto

penale e prospettive "de jure condendo". *Ciberspazio e diritto*, 2008.

Salvadori, I. L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking. *Rivista italiana di diritto e procedura penale*, 2008.

Sarzana di Sant'Ippolito, C. Sicurezza informatica e lotta alla cybercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislative. *Diritto dell'Internet*, 2005.

Sarzana di Sant'Ippolito, C. La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa. *Diritto penale e processo*, 2008.

Stracuzzi, A. Data retention: il faticoso percorso dell'art. 132 Codice Privacy nella disciplina della

conservazione dei dati di traffico. *Il Diritto dell'informazione e dell'informatica,*, 2008.

Thomas, D., e B. Loader. *Cybercrime: law, enforcemnt, secutiry and surveillance in the information age.* London: Routledge, 2000.

Wall, D. Cybercrimes and the internet. In *Crime and the Internet*, di D. Wall. London: Routledge, 2001.

Yar, M. *Cybercrime and society.* London: Sage, 2006.

## NOTES

[1] *Art. 615-ter. Accesso abusivo ad un sistema informatico o telematico.*
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

[2] *Art. 614. Violazione di domicilio.*
Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione fino a tre anni. Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha il diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno. Il delitto è punibile a querela della persona offesa. La pena è da uno a cinque anni, e si procede d'ufficio, se il fatto è commesso con violenza sulle cose, o alle persone, ovvero se il colpevole è palesemente armato.

[3] *Art. 615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.*
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

[4] *Art. 616. Violazione, sottrazione e soppressione di corrispondenza.*
Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

[5] *Art. 635-bis. Danneggiamento di informazioni, dati e programmi informatici.*
Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso com abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

[6] *Art. 635-ter. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.*
Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso com abuso della qualità di operatore del sistema, la pena è aumentata.

[7] *Art. 635-quater. Danneggiamento di sistemi informatici o telematici.*
Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con La reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso com abuso della qualità di operatore del sistema, la pena è aumentata.

[8] *Art. 635-quinquies. Danneggiamento di sistemi informatici o telematici di pubblica utilità.*
Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

[9] See note no. 3.

[10] *Art. 615-quinquies. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.*
Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

[11] *Art. 640-ter. Frode informatica.*
Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a ter anni e con la multa da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

[12] *Art. 495-bis. Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri.*
Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno.

[13] *Art. 640-quinquies. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.*
Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

[14] *Art. 600-quater.1. Pornografia virtuale.*
Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.