INFORMATION TECHNOLOGY & LAW SERIES 11

CYBERCRIME AND JURISDICTION

A Global Survey

edited by

Bert-Jaap Koops and Susan W. Brenner

contributions by

Susan W. Brenner
Roberto Chacon de Albuquerque
Noel Cox
Pavan Duggal
Peter Grabosky
Jessica R. Herrera-Flanigan
Paul de Hert
Gus Hosein
Henrik W.K. Kaspersen
Bert-Jaap Koops
Jeong-Hoon Lee
Fernando Londoño
Pauline C. Reich
Ulrich Sieber
Henrik Spang-Hanssen
Gregor Urbas
Ian Walden
Giovanni Ziccardi
Rodrigo Zúñiga

T•M•C•ASSER PRESS
The Hague

Chapter 11
CYBERCRIME AND JURISDICTION IN ITALY

Giovanni Ziccardi*

11.1 Substantive Cybercrime Law

11.1.1 The Constitution of 1948

The Italian Constitution, drawn up in 1948,[1] is the most important normative document in Italy that includes several specific provisions, contained in many articles, related to data-protection issues, the secrecy of private correspondence, warrants that must be granted during search and seizure, and civil-rights protection regarding any aspect of citizens' social lives.

These articles of the Constitution, of course, do not directly refer to the 'electronic world' – in 1948 the technological era was just beginning – but most of the principles explained in these articles can be extended. The Italian Courts, during the last twenty years, have done so several times with respect to cyberspace issues.

One of the most important articles of the Constitution – an article that Italian courts usually extend to cyberspace and to illegal-access issues – is Article 14. The text of this article is very plain: it states that a) the personal domicile is inviolable, and that b) inspections and searches may not be carried out except in cases, and in certain ways, laid down by law, in conformity with guarantees prescribed for safeguarding personal freedom.

We will see later on in this chapter that the notion of 'domicile', according to the Italian law, is very broad and is, at the same time, a place that is 'physical' and 'virtual'. The Italian Criminal Code (*Codice Penale*) regulates trespassing a virtual 'dwelling' (for example, the computer owned by a user, or an authentication device) in the same manner as trespassing physical doors and windows to get into a 'real' dwelling. The basic idea, in court interpretations during these years, is strictly

* Prof. Dr Giovanni Ziccardi is Professor of Legal Informatics and Advanced Legal Informatics at the Faculty of Law, University of Milan, Italy. Many thanks to Dr Nadina Foggetti for her co-operation during the draft of this chapter (especially the jurisdiction part).

[1] On 2 June 1946, after the public voted for a Republic in the referendum concerning the (future) form of the state, the Italian Constituent Assembly was elected. On 11 December 1947, the new Italian Constitution was passed, and it entered into force on 1 January 1948.

B-J. Koops and S.W. Brenner (Eds), Cybercrime and Jurisdiction

connected to the existence of a 'virtual' or 'electronic' domicile alongside the 'real' one.

The same principles apply to the contents of Article 15 of the Italian Constitution, which states that the liberty and secrecy of correspondence and of *every form* of communication are inviolable, and that limitations thereupon may only be enforced by a decision, for which sufficient grounds must be given, of the judicial authorities with the guarantees laid down by law.[2]

The notion 'every form of communication' in the Constitution is very broad and effective, and extends this high level of constitutional protection not only to the traditional physical – or 'snail' – mail, but also to 'virtual correspondence'. This includes not only, obvious though it may be, e-mail, but also non-public mailing lists and other forms of private transmission of data between individuals.

These two articles of the Italian Constitution have been the first to be applied in cases where the legislative framework did not have specific technological or cyberspace-related legal provisions. This legislative framework, however, was to change a great deal in the 1990s.[3]

11.1.2 **The first real informatic provisions**

The legislative framework related to computer crimes and cyber-investigations in Italy changed significantly during the years 1992 and 1993. The two most important legislative reforms in fact date from more than ten years ago. The first, Legislative Decree (*Decreto Legislativo*) No. 518 of 29 December 1992, modified the existing Italian Copyright Act (Law No. 633 of 1941). The second, Act (*Legge*) No. 547 of 23 December 1993, 'Replacements and introduction of new articles on computer crimes into the Criminal Code and into the Criminal Procedure Code' (*Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*), was enacted to modify the Italian Criminal Code and the Criminal Procedure Code (*Codice Procedura Penale*) and to introduce new provisions related to software piracy, computer crimes, and cyber-investigatons.[4]

11.1.3 **Copyright law**

The 1992 Decree No. 518 addressed copyright in the information age and software piracy. It became the heart of the Italian legislation protecting intellectual property

---

[2] For a concise but clear description in English of the legal framework of privacy in Italy, see Privacy International, 'Italian Republic', in *Privacy & Human Rights 2003*, Washington, D.C./London, available at <http://www.privacyinternational.org/survey/phr2003/countries/italy.htm>.

[3] See G. Livraghi, 'Internet freedom, privacy and culture in Italy (and the activity of NGO's)', 1 *Ciberspazio e Diritto* (2000) No. 1, pp. 21-30.

[4] See G. Pica, *Diritto penale delle tecnologie informatiche* [Criminal Law of the Information Technologies] (Turin, Giappichelli 1999).

and copyright. It was enacted to implement in Italy the European Community Directive 91/250 that provides software with the same protection as literary authorship. As two scholars, Monti and Livraghi, have written, this law defines the duplication of software for a 'lucrative purpose' as a criminal offense punished with a term of imprisonment from one to three years. The Decree was intended to repress the sale of illegal software copies in Italy, 'but it was interpreted in such a way as to criminalize even private and non-commercial exchanges.'[5]

The Copyright Act was subsequently modified and updated through several legislative reforms, during the years 2000, 2003, and 2005. These modifications concerned the punishment of 'new' forms of conduct, especially file-sharing, peer-to-peer systems, and circumvention of technological protection measures and digital rights management (DRM) systems.[6] These provisions essentially protect, in the current legislative framework, the integrity of copyrighted software, establishing penalties against selling pirated software and evading taxes on software.

11.1.4 **The Italian Computer Crimes Act of 1993**

The 1993 Act No. 547, in contrast to the copyright Decree that targeted copyright law, focused completely on criminal issues, updating the Italian Criminal Code (CC) and the Criminal Procedure Code (CPC) to punish also 'non-traditional' or 'virtual' conduct related to computer crimes.

This Act added several articles to the Italian Criminal Code, thus becoming the heart of the Italian computer-crime discipline. It is very complex, too broad and vague in some parts. It contains twelve points concerning many computer-related criminal activities, including illegal access to information systems, voluntary damage to information systems, trafficking of passwords and access codes, the creation and diffusion of viruses and worms,[7] and the creation of false electronic documents. It also includes a definition of 'computer crime': a computer crime, for the purposes of the Italian legislative system, is 'an offense committed by using computer technologies, from a personal one to portable telephone devices created on the basis of microchips.'

In combination with the copyright law, this Act provides, in Italy, government organizations, firms, military institutions, banks, companies, and private citizens

---

[5] For more information about this legislative evolution, see A. Monti, 'The network society as seen from Italy', paper presented at the Conference for Freedom and Privacy (CFP) 2000 in Toronto (6 April 2000), available at <http://www.cfp.org>.

[6] See Art. 71-*sexies*, Art. 102-*quater* of the Italian Copyright Act (Law No. 633 of 1941), derived from Art. 6 of the EC Directive 2001/29/EC concerning the obligation as to technological measures (the Member States shall provide adequate legal protection against the circumvention of any effective technological measures) and Art. 171-*ter* of the same Law.

[7] See Y. Amoroso Fernández, 'Virus informatici: aspetti legali' [Informatics Viruses: Legal Aspects], *Informatica e diritto* (1999) p. 217; G. Ziccardi, 'I virus informatici: aspetti tecnici e giuridici' [The Informatics Viruses: Technical and Legal Aspects], *Ciberspazio e diritto* (2001) Nos. 3-4, p. 347.

with protection from unauthorized access to computer networks, illegal use of protected data bases, unlawful copying of chip topographies, and unauthorized use of codes of credit and phone cards, passwords, or banking accounts.

The Italian Computer Crimes Act is divided into several parts, each one concerning different conduct and provisions. The first part, more specifically the first four articles, deals with the possession, alteration, or destruction of data or computer systems. These provisions are shaped on the basis of 'physical' counterparts, in this case the typical damage that can be encountered in the physical world (for example, someone who voluntarily damages someone else's car), extending these to information-technology objects – in this case, information systems and the data that are managed by those systems. The result of this extension is that someone who damages the data and computer systems of someone else is now also punishable.

The second part of the Act deals with unauthorized or pirated access to systems and with the interception of communications. Also in this case, the Italian legislator moves from the 'physical point of view' (the domicile, such as a house, and physical correspondence, for instance, a letter) to punish the trespassing of virtual property, i.e., the access to a system against the will of the owner, or the illegal interception or possession of private correspondence, either 'static', like an e-mail message, or 'dynamic', such as information flows and private chat conversations.

The third part of Act No. 547 of 1993 concerns forging an electronic transmission, spreading computer viruses, illegally possessing devices to intercept or disrupt communications, and disclosing confidential information. All these provisions carry penalties of up to six years' imprisonment.[8]

The first time these new norms were enforced was in 1994, when the Italian Finance Police started a massive operation, 'Hardware I', that was the first Italian operation concerning computer crimes and copyright violations.[9] It was a nationwide operation, and the results were the shutdown of hundreds of bulletin boards (BBSs) connected to the Fidonet network, alongside many seizures of hardware, software, blue boxes,[10] and other electronic devices.[11] It was the first time, in Italy, that the target of prosecutors and the police were the so-called 'telecom pirates': the

---

[8] For a brief description, in English, of the Italian computer crimes legal frameworks see, *inter alia*, Michael W. Kim, *How countries handle computer crimes* (1997), available at <http://www.swiss.ai.mit.edu/6.805/student-papers/fall97-papers/kim-crime.html>.

[9] See S. Chiccarelli and A. Monti, *Spaghetti Hacker. Storie, tecniche e aspetti giuridici dell'hacking in Italia* [Spaghetti Hackers. Stories, Techniques, and Legal Aspects of Hacking in Italy] (Milan, Apogeo 1997).

[10] 'An early phreaking tool, the blue box is an electronic device that simulates a telephone operator's dialing console. (…) The most typical use of a blue box was to get free telephone calls. Blue boxes no longer work in most western nations, as the switching system is now digital and no longer uses inband signaling.' See <http://en.wikipedia.org/wiki/Blue_box>.

[11] See C. Gubitosa, *Italian crackdown. BBS amatoriali, volontari telematici, censure e sequestri nell'Italia degli anni '90* [Italian Crackdown. BBS Lovers, Telematics Volunteers, Censorship, and Seizures in 1990s Italy] (Milan, Apogeo 1999).

main accusation made against the BBS users was that they downloaded, copied, and transmitted pirated software and that they trafficked data and passwords.

Comparable to the first wave of cybercrime legislation, the years 2000-2005 saw a second wave of legislative reforms, addressing new computer crimes, illegal content, child-pornography material, and the security of the e-commerce environment. For example, in 1998, the Italian Act concerning Child Pornography and the Internet, Act No. 269 of 3 August 1998, was enacted. Several projects have started to modify the original text, including a Bill approved by the Council of Ministers on 7 November 2003, and a self-regulatory initiative, the Codice di Autoregolamentazione 'Internet e minori' (Self-Regulation Code 'Internet and Minors'), is sponsored by many institutions, including the Italian Ministry for Innovation and Technologies. Other examples in this second wave are laws on copyright and related computer crimes,[12] laws concerning terrorism and wiretapping,[13] and a law concerning electronic commerce.[14]

I shall conclude this section by describing some of the most relevant cybercrimes under the Computer Crimes Act of 1993.

Illegal access to a computer system

The conduct which amounts to illegal access to a computer system is clearly defined in the text of Article 615-*ter* CC, carrying a penalty of one to three years' imprisonment for 'anyone who enters without authorization a computer or telecommunication systems protected by security measures, or who remains in the system against the expressed or implied will of the one who has the rights to exclude him.'

As, among others, the scholars Pica and Foggetti have noted in several of their studies,[15] the content of Article 615-*ter* and the other offenses introduced by Act No. 547 of 1993 was drafted using the offense of trespassing (violation of domicile) as defined in Article 614 CC as a model. As noted above, the Act tends to identify new forms of unlawful conduct as different kinds of aggression against traditional legal rights, but it does not consider computer crimes as a new and independent category that needs to be defined on the basis of new legal rights to be protected.[16] The Explanatory Report to Act No. 547 of 1993 clearly shows the legislator's intention to protect in the definition of illegal access 'an extension of the sphere pertaining to each individual, which is safeguarded by Article 14 of the Constitution as well as by Articles 614 and 615 of the Criminal Code.'[17]

---

[12] Act of 18 August 2000, No. 248; Legislative Decree of 9 April 2003, No. 68; Act of 21 May 2004, No. 128; and Act of 31 March 2005, No. 43.

[13] Decree of 18 October 2001, No. 374, and Decree of 27 July 2005, No. 144.

[14] Legislative Decree of 9 April 2003, No. 70.

[15] See N. Foggetti, 'Legal analysis of a case of cross-border cyber crime', IV Upgrade, European Journal for the Informatics Professional (2003) No. 6, p. 43, available at <http://www.upgrade-cepis.org; Pica> (1999) op. cit. n. 4.

[16] See Foggetti, loc. cit. n. 15, p. 43.

[17] Ibid.

Concerning the nature of the security measures that are an element of the criminal provision, Foggetti notes that prevailing case law considers that, while being a constituent element of the concept of illegal access to a computer system as defined in Article 615-*ter* CC, these measures need only show the will of the owner of a specific system to be protected – they do not have to be really efficacious in a technical sense. In other words, such measures are not considered so much in terms of how suitable they are to keep out any intruders, but rather as a way of declaring the 'right to exclude others' (*ius excludendi alios*), in parallel with the legislation that governs the physical domicile (Art. 614 CC).[18]

The same law includes a series of aggravating circumstances that affect the prosecution of the offense, allowing the maximum penalty to be raised to five years, for example, when the system is serving the public interest, or when the intruder is the system administrator of the network.

Illicit possession of access codes

Another very important provision is Article 615-*quater* CC, which defines illicit possession of access codes to information and telematic systems as an offense. This article carries a penalty of up to one year's imprisonment and a fine of up to around 5,000 Euro for 'whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally acquires, reproduces, propagates, transmits, or delivers codes, keywords, or other means for access to a computer or telecommunication system protected by security measures, or provides information or instructions fit to the above purpose.'[19] It is interesting that for this offense, no actual damage or disruption to the system has to be caused.

11.1.5 **The Data Protection Acts of 1996 and 2003**

In 1996, a law concerning the protection of personal data was enacted, the Italian Data Protection Act.[20] This Law, No. 675 of 1996, implemented the European Community Data Protection Directive. It was completely modified in 2003 with a brand new 'Italian Privacy Code', enacted through Legislative Decree No. 196 of 2003. This Code protects the privacy and integrity of personal data and penalizes the illegal processing of this kind of data. It is enforced by the Italian Data Protection Authority ('Garante').

From a cybercrime perspective, an interesting provision in the Italian privacy law is the obligation to adopt suitable and preventive security measures aimed at

---

[18] Ibid. Cf., Corte di cassazione, 6 December 2000 No. 12732.

[19] See Foggetti, loc. cit. n. 15, p. 43.

[20] See J. Monducci, 'La circolazione dei dati personali in Internet' [The Dissemination of Personal Data on the Internet], 1 *Ciberspazio e Diritto* (2000) No. 1, pp. 31-40.

preventing the loss or destruction of personal data and unauthorized access to personal data.[21]

11.2 Procedural Cybercrime Law

11.2.1 **Network wiretapping**

Wiretapping is regulated by Articles 266 to 271 of the Italian Criminal Procedure Code (hereafter: CPC). It can only be authorized in the case of legal proceedings, and government interceptions of telephone and all other forms of communications must be approved by a court order. They are granted for crimes punishable by life imprisonment or imprisonment for more than five years, for crimes against the administration punishable by no less than five years' imprisonment, for crimes involving the trafficking of drugs, arms, explosives, and contraband, and for insults, threats, abuses, and harassment carried out over the telephone. The government interception powers have their counterpart in the Computer Crimes Act, which contains a provision that penalizes the interception of electronic data flows.[22]

The procedural articles are also used for the interception of communication between two modems, especially through Article 266-*bis* CPC that provides for network wiretapping. Before the Computer Crimes Act of 1993, only telephone interception was allowed and only in cases of serious crimes (such as arms or drugs trafficking or usury) as well as only with the authorized instruments of the inquiring authorities. Some scholars noted that the new legislation introduced a general and undefined concept of network wiretapping that can be used for any suspected crime or violation that uses information or network technologies, and that the interception can be carried out by any means including privately-owned equipment, creating a practically unlimited and unrestricted right of interception.[23]

11.2.2 **Search, seizure, and network searches**

The procedures that can be used by the police to investigate a computer or a network are the same as the Criminal Procedure Code provides for searching persons or places. These are called instruments of evidence (*mezzi di prova*) and are laid down in Articles 244 through 271 CPC. In particular, there are four instruments used by the police to search for evidence on a computer or a network: inspection

---

[21] See G. Corasaniti, *Esperienza giuridica e sicurezza informatica* [Legal Experience and Informatics Security] (Milan, Giuffrè, 2003); P. Perri and S. Zanero, 'Lessons learned from the Italian law on privacy', 20 *The Computer Law and Security Report* (2004) Nos. 4-5.

[22] For a brief description of these issues in English, see Privacy International, loc. cit. n. 2.

[23] A. Monti, 'Diritto delle tecnologie dell'informazione e protezione dei diritti civili' [Information Technology Law and Protection of Civil Rights], 1 *Ciberspazio e Diritto* (2000) No. 1, pp. 41-51.

(*ispezione*), search (*perquisizione*), seizure (*sequestro*), and tapping (*intercettazione*). All these four instruments can be used to search persons, places, computers, networks, and communications for evidence.

If the investigation of, for example, a network would cross the Italian border, there are various options, depending on the state towards which the investigative activity must be performed. Like with ordinary crimes, in the case of a computer crime, the general rules for assistance through Interpol or, if the state is in the EU, for Europol can be applicable; and for countries that have ratified the Council of Europe Convention on Cybercrime (Budapest, 23 November 2001) – not necessarily members of the Council of Europe –, legal assistance will be possible through the provisions of that convention. For investigation activities within the EU, moreover, the EU Convention on Mutual Legal Assistance can be used for computer crimes as well, together with the general procedures of extradition and the European arrest warrant.

11.2.3 **Data retention**

In 2004, a law concerning data retention was enacted, Law No. 45 of 26 February 2004, which is very important from a cyber-investigation point of view. It was partially reformed by the Law of 31 July 2004, No. 155, issued to prevent terrorism activities. It contains the obligation to retain log files concerning telephonic conversations for a period of 24 months, plus a further 24 months to prevent or verify crimes. During the first 24 months, data are stored by the provider and can be accessed after a court order; during the second 24-month period, data can only be accessed if there is a crime related to terrorism, organized crime, or damage to information systems. This law can not be used for electronic (telematic) data flows, but only for telephone communication systems and telephone data.

11.3 Jurisdiction: the Applicability of Italian Criminal Law

11.3.1 **The *Locus Commissi Delicti* Issue**

Obviously, the thing that distinguishes cybercrime from other criminal activities is basically the cross-border nature of unlawful conduct over the Internet. It is not always feasible to identify the *locus commissi delicti* (the place where the offense was committed) when the offender makes use of informatic and telematic means to commit the offense, as the same single criminal act often involves many different activities that are carried out via several intermediate systems or stepping-stones.[24] The attacker may, in fact, violate several computer systems with just one act of illegal access and carry out several illegal operations on computers that are inter-

[24] See Foggetti, loc. cit. n. 15, p. 46.

connected but physically located in different territories, sometimes in different countries. In other cases, the place where the initial violation occurs may be the same as the place where the attacker is located, but the person harmed by the offense may be somewhere else.

11.3.2 The obligatory nature of Italian criminal law

The first problem is to determine whether or not Italian law can be applied to a particular event. Article 3 of the Italian Criminal Code, entitled 'Obligatory nature of the criminal law' (*Obbligatorietà della legge penale*), defines the principle that the penal law is imperative, except for the temporal and spatial limits stated by national law. According to Article 3 CC, 'Italian criminal law applies to all citizens or foreigners within the territory of the state, save for those exceptions provided for by national public law or international law.' Article 3 paragraph 2 adds: 'Italian criminal law also applies to all citizens or foreigners who are abroad, but limited to those cases provided for by that same law or by international law.'

The obligatory nature, as Foggetti states, is also expressed in the position of the article itself within the system of the Criminal Code, as it, in fact, comes before the norms referring to the territorial application of criminal law and the principle of *ignorantia legis non excusat* (ignorance of the law is no excuse), and coming after the principles of legality and the norms referring to *ratione temporis* (time limitations governing the applicability of criminal law).

Article 3 determines the non-derogable nature of the application of Italian criminal law based on personal (*ratione personae*) jurisdiction, whereby it is applicable to all persons – whether Italian citizens or foreigners, whether in the national territory or abroad –, the only limitations being the principle of legality and the norms laid down by international law.[25]

11.3.3 The principle of territoriality

The principle of territoriality is dealt with in Article 6 paragraph 1 CC, which defines criminal law as being applicable within the whole territory of the Italian state. It is therefore essential to define where the offense was committed. Article 6 paragraph 2 provides that the 'offense is considered to have been committed within the territory of the state when the action or omission giving rise to the offense is carried out fully or partially there, or if the consequence of the action or omission was suffered there.'

The Italian Criminal Code, therefore, aims to expand the jurisdiction of Italian criminal law by establishing a criterion of ubiquity, with the origin or the result occurring in Italy. This raises the question of how to define the 'slightest part' of a criminal act that can cause the offense to be considered as having been committed

[25] Ibid., p. 46.

in Italy. The resulting problem of interpretation has found no unanimous solution at a doctrinal level and also creates divergences in case law.[26]

Among legal scholars, there has been much debate about the minimum significance of an activity committed within Italian territory in order for Italian law to be applicable. One interpretation holds that acts committed within the national territory should constitute a punishable attempt and not be limited to a mere preparatory act, or even that the offense should be considered as having been committed in Italy even though only a 'fragment' of the offense, or even a mere preparatory act, was committed in Italy. This doctrine holds that a criminal attempt can be considered to have been committed in Italy even though the preparatory acts may not have been committed in Italian territory, provided that the unlawful act could potentially have been committed within the Italian territory.

Conversely, according to another criterion based on a literal interpretation of the norm, the offense should be considered as coming under Italian jurisdiction only when a part of it, whether completed or attempted, has been committed in Italian territory, provided that the 'part' was an essential component of the offense. Such a decision must be taken after the event (*ex post*) and in relation to the specifics of the case, and not merely before the event (*ex ante*) and abstractly. Prevailing case law seems to accept this latter interpretation.[27]

With regard to the minimum requirements to consider an offense as attempted, for the purposes of applying Italian jurisdiction in compliance with Article 6 paragraph 2, prevailing case law consider that 'the part of the act committed in Italy does not in itself have to be actionable but it is enough that the part of the act which was committed in Italy, in conjunction with subsequent unlawful actions committed abroad, could be considered as an attempted or completed offense.' This interpretation would seem to accept the theory of the 'potential commission of the deed'. However, the same ruling[28] continues with a restrictive interpretation requiring that 'an attempted criminal act carried out in Italy must have some corresponding objective impact on the outside world.'

11.3.4 **Applicability of the principle of territoriality**

The criterion of ubiquity is particularly useful to apply to offenses committed over the Internet. The main doctrine on the subject considers that Italian jurisdiction should apply when the data involved in the offense, although they may have been put on the Internet outside Italy, pass through servers located in Italy, or when the storage and copying of the data has taken place in Italy.[29]

---

[26] Idem, p. 44.

[27] Idem, p. 45.

[28] Corte di cassazione, Sezione I, 20 March 1963, *Rivista italiana di diritto e procedura penale* 1965, p. 118 et seq.; Corte di cassazione, Sezione IV, 22 February 1993, *Giustizia penale* 1993, II, n. 517, p. 629.

[29] See Foggetti, loc. cit. n. 15, p. 46.

The principle of ubiquity is specifically applicable in cases of defamation over the Internet. Italian case law states that, on the basis of that principle, an Italian judge can try such an offense, either if it has been committed in national territory or if the *iter criminis* (crime route) was initiated abroad but has been completed, resulting in a crime, in Italy.[30]

11.3.5 **Applicability of the principle of defense**

For the applicability of Italian criminal law, as an alternative to the principle of territoriality, our judicial system provides for the application of the 'principle' of defense, through which the criminal law can be applied not on the basis of where the offense was committed or of the nationality of the offender, but rather on the basis of who the victim of the offense was.

Thus, according to this principle, Italian criminal law is applicable if the offense was committed against the Italian state or against an Italian citizen, regardless of where it was committed. Article 10 CC states that a foreigner who 'commits, in a foreign territory, against the Italian state or against an Italian citizen, an offense for which Italian law specifies life imprisonment or a custodial sentence of no less than a year, will be punished under that law.' This article is a corollary of Article 3 CC, by which Italian law is universally obligatory, unless it is limited by conflicting national or international laws.

Whether an unlawful conduct committed by a foreigner in a foreign territory can be punished under Italian law will also, however, depend on some other conditions: the offender must be present in Italian territory and there must be either a petition from the Italian Ministry of Justice or a lawsuit or complaint by the offended party (Art. 10 para. 1 CC).

Another possibility is provided by Article 10 paragraph 2 CC. If an offense harms the European Community, a foreign state, or a foreigner, the perpetrator can be prosecuted according to Italian criminal law if (and only if) (1) he or she is in Italian territory; 2) the crime carries a penalty of imprisonment for life or not below three years, and (3) if extradition was not granted or was not accepted by the state's government where the crime was committed or the government of the perpetrator's state.

11.4 A Typical Case: an Attack from 'Outside'

The scholar Foggetti describes, in several studies, in relation to the problem of applicable law, a typical cross-border cybercrime case that actually occurred, although it has not yet been tried in court.[31]

---

[30] Ibid., p. 48. One of the most important decisions here is Corte di cassazione, 29 April 1980, *Cass. Pen. Mass. Ann.* 1981, p. 1558.

[31] Ibid., p. 46.

The case concerns a Swiss hacker who violated a public-interest information system in Switzerland, affecting and damaging Italian users connected to the compromised system. The system attacked was of 'public interest', since thousands of users from all over the world were connected to it, and because experiments were conducted and analyzed using the hardware and software resources located in Geneva. The hacker made use of a local vulnerability of the system, and he upgraded his privileges from 'normal user' to 'root user'.

He went on to install a rootkit, which made the attack a Trojan-like attack, and very complex software, including a 'sniffer', in order to copy the passwords keyed in on-line, and he installed other programs with backdoors that could later be used to get back into the system without having to trespass and break it again. The rootkit also contained some tools to hide any trace of the attack, by altering the system commands that enable the intrusion to be verified, thereby canceling the activity logs.

The attack was launched from Geneva, but the copied passwords belonged to Italian users who were connected to the violated system. The hacker thus committed the crime in Switzerland, compromising the integrity of a computer system there, but he 'cracked' the passwords of user subscribers who connected to the system from Italy. Even though the passwords were keyed in by Italian users, from computers located on Italian territory, the 'minimum requirement' needed for Italian law to apply was *not* fulfilled: the deed of 'copying the passwords' was done wholly in Geneva, and also the rootkit was installed in the Geneva machines. In this case, the territoriality principle cannot be applied in order to determine whether the offense is punishable under Italian law.

Moreover, the principle of defense, explained in the above-mentioned Article 10 CC, was not applicable, since the Italian users had not filed a lawsuit or complaint against the hacker. Likewise, none of the conditions of Article 10 paragraph 2 were fulfilled. Therefore, the case was not punishable under Italian law, and the Swiss law was fully applied.

This would have been different if the rootkit had been installed on an Italian machine, located on Italian territory. In that case, the violation of an Italian system would have constituted the final link in the attacker's criminal project, and Italian criminal law could have been applied, not by virtue of the principle of the nationality of the offended party, but based on the criterion of ubiquity as set out in Article 6 paragraph 2 CC. The attack would then have implied the 'minimum necessary requirement' to allow the entire illegal conduct to be tried under Italian law.

11.5 Conclusion

As we have seen, the Italian legislator has preferred to use the categories of old crimes to discipline computer crimes, and this is probably the main reason for some interpretative problems that are often faced by the Supreme Court.

The criteria for cybercrime jurisdiction are the same as those used in general criminal law, notably the territoriality principle, or the *locus commissi delicti* principle, and the principle of defense. For this reason, one could talk of an adaptation of old principles to new technologies. These principles can be used, with some limitations, to fight cybercrime.

It is very important, given the nature of cybercrime, to regulate investigative activities beyond state borders. The Convention on Cybercrime is a perfect example of an attempt to do this, but the slowness of ratification shows how difficult it is for many states to accept a limit to their sovereignty.

Bibliography

Y. Amoroso Fernández, 'Virus informatici: aspetti legali' [Informatics Viruses: Legal Aspects], *Informatica e diritto* (1999) p. 217.

S. Chiccarelli and A. Monti, *Spaghetti Hacker. Storie, tecniche e aspetti giuridici dell'hacking in Italia* [Spaghetti Hackers. Stories, Techniques, and Legal Aspects of Hacking in Italy] (Milan, Apogeo 1997).

N. Foggetti, 'Legal analysis of a case of cross-border cyber crime', IV *Upgrade, the European Journal for the Informatics Professional* (2003) No. 6, p. 43, available at <http://www.upgrade-cepis.org>.

C. Gubitosa, *Italian crackdown. BBS amatoriali, volontari telematici, censure e sequestri nell'Italia degli anni '90* [Italian Crackdown. BBS Lovers, Telematics Volunteers, Censorship and Seizures in 1990s Italy] (Milan, Apogeo 1999).

G. Livraghi, 'Internet freedom, privacy and culture in Italy (and the activity of NGO's)', 1 *Ciberspazio e Diritto* (2000) No. 1, pp. 21-30.

A. Monti, 'The network society as seen from Italy', paper presented at the Conference for Freedom and Privacy (CFP) 2000 in Toronto (6 April 2000), available at <http://www.cfp.org>.

A. Monti, 'Diritto delle tecnologie dell'informazione e protezione dei diritti civili' [Information Technology Law and Protection of Civil Rights], 1 *Ciberspazio e Diritto* (2000) No. 1, pp. 41-51.

C. Parodi, 'Profili penali dei virus informatici' [Criminal Profiles of the Informatics Viruses], *Diritto penale e processo* (2000) No. 5, p. 632.

G. Pica, *Diritto penale delle tecnologie informatiche* [Criminal Law of Information Technologies] (Turin, Giappichelli 1999).

G. Ziccardi, 'La libertà di espressione in Internet al vaglio della Corte Suprema degli Stati Uniti' [Freedom of Expression on the Internet under the Scrutiny of the U.S. Supreme Court], *Quaderni Costituzionali* (1998) No. 1, pp. 123-134.

G. Ziccardi, 'I virus informatici: aspetti tecnici e giuridici' [Informatics Viruses: Technical and Legal Aspects], *Ciberspazio e diritto* (2001) Nos. 3-4, p. 347.

G. Ziccardi, *Crittografia e Diritto* [Cryptography and Law] (Turin, Giappichelli, 2003).