# Control of file exchange of illicit materials in peer-to-peer environments

*Cesare Maioli and Michele Ferrazzano*
*CIRSFID and Faculty of Law*
*University of Bologna*



*Keywords:* Legislation on computer-crimes, Convention on Cybercrime, Child pornography, Peer-to-peer networks, Forensic tools

## 1 HARMONIZATION OF LEGISLATIONS AGAINST COMPUTER-CRIME

The fast developments in the field of information technology have given rise to unprecedented economic and social changes on all sections of modern society, The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opened a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, the cyberspace, which is used for legitimate purposes but may also be the subject of misuse. Thus a dark side [Walden, 2007]: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. The simple example of the spread of detrimental computer viruses all over the world has provided proof of this reality. The implementation of technical measures to protect computer systems is needed concomitantly with legal measures to prevent and deter criminal behaviour which either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.

### 1.1 The Emergence of Cybercrime

There is no agreed definition of what constitutes a computer crime. According to accepted definitions of the state [Walden, 2007] a computer may constitute the instrument of the crime, such as in identity theft and forgery; the object of the crime, such as the theft of processor chips; or the subject of the crime, such as hacking or cracking. The involvement of computers may challenge traditional criminal concepts, such as fraud, as well as facilitating particular types of crime, such as child pornography or criminal copyright infringements; In general such inappropriate and misuse of content are related to the use of ICT to facilitate the distribution of unlawful contents or illegal data. The computer may be the subject of the crime and with laws that have been established to

specifically address activities that attack the integrity of computer and communications networks, such as the distribution of computer viruses.
The difference between the categories is mainly one of focus; in all of them the computers are a tool for the commission of a crime, rather than the target itself. However in computer-related crime the information being processed is also an instrument for committing a criminal act, while in content-related crime, the information is the crime, not a tool.
The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Whilst international measures, starting with Recommendation No. (89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems, resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology, should be addressed.

**1.2 The Coordination of Initiatives**

ICT and cybercrime have an obvious international dimension and governments have recognized the need to ensure that legal protection is harmonized among nations [Walden, 2004]. Attempts have been made within various international organizations and institutions, such as G8, the ASEAN states and the United Nations, to achieve a harmonized approach to legislating against computer-crime and thereby try to prevent the appearance of computer-crime havens. The first major attempts was under the auspices of the Organization for Economic Cooperation and Development which in 1986 published a report listing the categories of offences that it was believed should constitute a common approach to computer-crime. Harmonization initiatives have tended to address both substantive offences and criminal procedures; for the former, national legal traditions have generally proved a greater barrier to harmonization than in the field of criminal procedures, due to the unavoidable effect that national criminal codes exhibit a variety of means of conceiving an activity that are not present when considering the process of investigation; for the latter national differences tend to be more principle-based, reflecting cultural concern about privacy and the proper limits of police powers.
The most significant institutions in the field have been the Council of Europe and the European Union. The Council of Europe in 1989 produced the report Computer Related Crime, the first guidelines for national legislatures on a set of list of offences necessary for a uniform criminal policy on legislation concerning computer-crime problems; this list included: computer fraud, computer forgery; damage to computer data or computer programs; computer sabotage; unauthorised access, unauthorised interception; unauthorised reproduction of computer programs; unauthorised reproduction of topography; these offences were seen by all Member States to be critical areas of computer misuse that required provisions in criminal law. In 1995, the Council of Ministers adopted a recommendation addressing issues of search and seizure, the admissibility of evidence and international mutual assistance with concern to procedural law connected with information technology.
But the Council of Europe Recommendations have not a binding power and therefore their effect is limited. However the growth of the Internet as a transnational environment for the commission of crime have refocused the attention of policy makers on the need for harmonized criminal law in the area; therefore in 1997 the Council started its work on the adoption of a Convention in the area, which Member States would have an obligation to implement: in November 2001 the Convention on Cybercrime was opened for signatures in Budapest and has since been signed by 47 members of the Council of Europe with 17 of them not yet followed the ratification.

The involvement of four important non-members (United States, Japan, South Africa, Canada) in the drafting process and the provision of a mechanism whereby other non-member can adhere and ratify the convention were important recognition of that work. The Convention entered into force on 1 July 2004.
The Convention addresses issues of substantive and procedural criminal law, which Member States area obliged to take measure to implement in national law, as well as issues of international cooperation. The comprehensive nature of the Convention, as well as the geographical spread of its signatories, means it is likely to remain the most significant international legal instrument in the field for many years from now [Walden, 2007]. Other intergovernmental organizations have also endorsed it suggesting the implementation of its principles. In 2005, the international police organization Interpol adopted a resolution recognizing that the Convention provides a minimal international legal and procedural standard and recommending its 182 member countries to consider to join it. Other harmonization initiatives were launched after the Convention in non European countries (e.g. Commonwealth).
Other important international organizations have been working with harmonization purposes: it is the case of the G8 which adopted in 1999 a set of principles on transborder access to stored data and after September 11 2001; G8 adopted a formal Recommendation on transnational crime which addressed the three categories of cybercrime and in which all G8 members confirmed (only for Russia it was an original statement) their intention to become parties to the Convention on Cybercrime.
Also the United Nations (UN) have always been concerned with the computer-crime through its agencies, e.g. ITU and Unicef, while only in two occasions the General Assembly expressed resolutions on computer-crime: in 1990 and in 2001 making general recommendations with regard to the need to eliminate safe havens and to improve cooperation between law enforcements agencies. In 2005, at the UN Congress on crime prevention and criminal justice, it was stated that UN are building a UN Convention on Cybercrime on the achievements of the work by the Council of Europe.
In terms of European Community policy initiatives, since 1999, the Action Plan to create an Area of Freedom, Security and Justice noted that computer fraud and offences committed by means of the Internet were candidates for measures establishing minimum rules relating to the constituent elements and penalties. While computer-crime was identified as an area that may be best combated by a European approach. Subsequently, at a special meeting of the European Council, Member State governments agreed that efforts should be made to reach common positions with respect to definitions of criminal offences and appropriate sanctions for particular areas of crime, including computer-crime. Subsequently, the Commission adopted a Communication on computer crime that included proposals for legislative measures in the area, such as the proposed Framework Decision (Creating a Safer Information Society) as well as a Communication on Network and Information Security, which addresses measures to prevent computer-crime.

### 1.3 The Convention on Cybercrime

One of the most important challenges in the fight against computer-crime and cybercrime is the difficulty for the police, judicial, administrative and other law enforcement authorities, not only in identifying the cyber criminals, but also in determining the focus, place and time of the execution of the crime. It is also very difficult to determine the extent and impact of the criminal acts committed through the new technologies.
The principal reason is represented by the great possibility for the offenders to be almost completely anonymous in the cyberspace. Secondly it depends on the characteristic volatility of electronic data and evidence which can be altered, deleted or erased. In order to warrant the success of the investigations, it is extremely important to therefore assure the speed and secrecy of the investigative techniques and the international cooperation between the national competent authorities.

The Convention has adapted the traditional procedural measures (i.e. search, seizure, interception) to the new technological environment. Nevertheless, the technological revolution facilitates the possibilities to share data, information and communication through the electronic highways, giving more opportunities to the offenders to commit illegal acts in the cyberspace. The development of the network of communications has opened new doors for the cyber criminals, changing not only the traditional commission of the crimes but also some substantial aspects of the criminal law and criminal procedure. That has led the Council of Europe to introduce some new procedural measures [Picotti, 2008]. In particular, the Convention contains specific provisions concerning the collection of evidence in electronic form, the expedited preservation of computer and traffic data (article 16), the production order (article 18), the real-time collection of traffic data (article 20) and the interception of content data (article 21).

When becoming a signatory or depositing an instrument of ratification, a state may make various declarations that it intends to meet its obligations through the requirement of additional elements, the possibility of which is provided for under the terms of article 40. States may also make reservations but only when the option exists in respect of an article.

The Convention contains a specific mechanism for periodic consultation between the parties concerning implementation issues, legal, policy and technological developments and possible amendment.

The Convention aims principally at: (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime; (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; (3) setting up a fast and effective regime of international co-operation.

The Convention, accordingly, contains four chapters: I) Use of terms; II) Measures to be taken at domestic level, substantive law and procedural law; III) International co-operation; IV) Final clauses. It consists of a Preamble, 47 articles grouped in IV Chapters (Use of terms, Measures to be taken at the national level, International Cooperation, Final provisions). Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer-crime or computer-related crime: it first defines nine offences grouped in four different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: 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 neighbouring rights. Section 1 refers to Offences against the confidentiality, integrity and availability of computer data and systems; examples, following articles 2 to 6, are illegal interceptions, data interference, system interference, misuse of devices. Title 2 refers to Computer-related offences; examples, following articles 7 and 8, are forgery and frauds. Title 3 refers to Content-related offences; example, following article 9, is child pornography. Title 4, article 10, refers to Offences related to and infringements of copyright and related rights. Moreover, article 11 addresses related liability issues in relation to attempts and aiding or abetting while article 12 addresses corporate liability.

Section 2 of Chapter II, about procedural law issues, has the aim to go beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form; it determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter, and then sets out the following procedural powers: expedited preservation 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. Chapter II ends with the jurisdiction provisions.

Section 2 address procedural provisions that Member States are obliged to implement in national law. These include: measures to enable the expedited preservation of stored computer data, following article 16; expedite preservation and partial disclosure of traffic data, following article 17;

the production and search and seizure of computer data, following articles 18 and 19; the real-time collection of traffic data, following article 20; the interception of content data, following article 21.
Section 3, with article 21, covers the issue of jurisdiction (article 22). In terms of international co-operation, the Convention addresses issues of extradition (article 24), mutual legal assistance between national law enforcement agencies (articles. 25-34) and the establishment of a 24/7 (24 hours per day, 7 days per week) network of points of contact to support such assistance (article 35).
Section 3 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 parties - 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-crime or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II.
Finally, Chapter IV contains the final clauses, which with certain exceptions repeat the standard provisions in Council of Europe treaties.

Once ratified, most of the European countries (such as Belgium, Germany, Italy and Spain) have placed the computer related offences close to the traditional offences, such as forgery, fraud or damage. In particular they have taken their structure as a model for the cybercrime provisions, where possible [Picotti, 2008]. These countries have placed the cybercrime provisions within the Criminal Code. Other States have placed the cybercrime provisions within a specific Law, such as a "Computer Crime Act". It is the case for example of Cyprus, India, Sri Lanka, Portugal, United Kingdom, Romania and Portugal and other common law countries. Both of these legal choices could be adequate in order to implement fully the Convention on Cybercrime. Nevertheless there is a wide agreement that the countries that have placed the cybercrime provisions into their Criminal Code have had more problems to typify the provisions due to the necessity to find a right balance with the traditional provisions (e.g. fraud, forgery, illegal interception).

As mentioned above, Chapter III contains a provision on a specific type of transborder 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 Parties. The set up of the 24/7 network is very important: effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in the Convention is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under this articles, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings, in particular as defined under article 35, paragraph 1, letters a) to c). It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer-crime or computer-related crime [COE, 2001].
Each Party’s 24/7 point of contact is to either facilitate or directly carry out the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer-crime or computer-related crime, yet other choices may be appropriate. Paragraph 2 provides that among the critical tasks to be carried out by the 24/7 contact is the ability to facilitate the rapid execution of those functions it does not carry out directly itself.

Moreover, paragraph 2 requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis. Paragraph 3 requires each point of contact in the network to have proper equipment. and the personnel participating as part of a Party's team for the network to be properly trained regarding computer-crime or computer-related crime and how to respond to it effectively
Since the adoption of the Convention in 2001, an additional protocol to the Convention was agreed by member states, concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems.

## 2 CHILD PORNOGRAPHY IN THE INTERNET

If any topic is unequivocally associated in the minds of politicians, the media and the public with the dark side of the Internet, it is that of child pornography. The Internet has facilitated the supply of this form of illegal content to such an extend that it is now considered a multimillion dollar industry primarily through a proliferation of pay-per-view sites, while at the same time, cyberspace engenders broader child protection concerns about the harms children can suffer from the content and contact available over the Internet [Walden, 2007]. As a consequence, child protection is currently in the forefront of governmental policy on cybercrime. Also if some of the images are taken surreptitiously without direct interference with the child, the vast majority of hard core images involve the direct abuse of children. It has been noted that the tremor pornography is inappropriate in the context of children since the term embrace a semi-legitimate industry and crates confusion in the minds of the public, especially where the images involve pubescent children. It is more appropriate the term child abuse. While the majority of children are abused by those related to them or in some form of relationship with them, the Internet provides a new environment for potential abusers to form intimate relationship with children at a distance, eventually leading to the arrangement of physical meeting with the child [Wall, 2009].

The Internet is seen as raising a wide range issues for child safety and protection, which can be broadly distinguished into concerns about the contents available to children over the Internet, and concerns about the use of the Internet to abuse children, specifically child pornography. Both aspects has been the subject of initiatives at EU level starting from the 1996 Commission Communication, COM(1996)487, on illegal and harmful content on the Internet, which was endorsed by the Parliament and Council.
In 2000, the Council decision 2000/375 was adopted: it required Member States to take measures to encourage and enable Internet users to report suspected child pornographic images, as well as promoting the effective investigation and prosecution of perpetrators, at national level and through Member State cooperation.
Article 9 of the Convention, 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.
In 2004 the Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography represented a more prescriptive measure and it harmonized the substantive law of Member States. Child pornography is conceived broadly to include 'realistic images of non-existent child', which differentiates the position in Europe from that in the US. However Member States are given the option of excluding the production and possession of such images from criminal liability where it is solely for the person's private use, where presumably the harm is considered to be of minor relevance [Walden, 2004]. The Decision requires Member States to criminalize both the sexual exploitation of children and child pornography. The former addresses the abuse that occurs in the production of pornographic images, although it is drafted broadly covering other forms of exploitation.

In respect to child pornography, four types of activity should comprise the offence: production; distribution, dissemination and transmission; supplying and making available; acquisition and possession [Clough, 2010]. By groping acquisition with possession the Decision potentially avoid a blur between the act of production and possession due to the process of downloading being equated to the offence of making available the illicit materials.

Article 9 of the Convention, covering offences related to child pornography states that:
*1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium.*
*2. For the purpose of paragraph 1 above, 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; c) realistic images representing a minor engaged in sexually explicit conduct.*
*3. For the purpose of paragraph 2 above, the term "minor" shall include ali persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.*
*4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d. and e, and 2, sub-paragraphs b. and c.*

This provision responded to the preoccupation of Heads of State and Government of the Council of Europe and corresponds to an international trend that seeks to ban child pornography, as evidenced by the adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).
This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalised 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. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.
Considering point 1, paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system. This provision was felt necessary to combat the dangers described above at their source [COE, 2001]. Paragraph 1(b) criminalises the ‘offering’ of child pornography through a computer system. ‘Offering’ is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. ‘Making available’ is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system. ‘Distribution’ is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of 'transmitting' child pornography. The term ‘procuring for oneself or for another’ in paragraph 1(d) means actively obtaining child pornography, e.g. by downloading it. The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such

material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.
Considering paragraph 2, the term 'pornographic material' is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which are capable of conversion into a visual image [COE, 2001].
A 'sexually explicit conduct' covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer. When the Convention adopt the broad formulation 'child pornography' it makes reference to: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realist images representing a minor engaged in sexually explicit conduct." It can be noted that the second category does not directly result in harm to a child, as potentially with the third category where an image can be entirely generated by a computer. However, the concern is that such images' might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture. favouring child abuse. The EU Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography defined child pornography in terms that reflect the Convention formulation.
Considering paragraph 3 it contains the definition of the term 'minor' in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a 'child' in the article 1 of the UN Convention on the Rights of the Child. It was considered an important policy matter to set a uniform international standard regarding age. It should be noted that the age refers to the use of (real or fictitious) children as sexual objects, and is separate from the age of consent for sexual relations. Nevertheless, recognising that certain States require a lower age-limit in national legislation regarding child pornography, the last phrase of paragraph 3 allows Parties to require a different age-limit, provided it is not less than 16 years.
Considering paragraph 4, there is the permission for Parties to make reservations regarding paragraph 1(d) and (e), and paragraph 2(b) and (c). The right not to apply these sections of the provision may be made in part or in whole. Any such reservation should be declared to the Secretary General of the Council of Europe at the time of signature or when depositing the Party's instruments of ratification, acceptance, approval or accession, in accordance with article 42.

In the case of Italy [Picotti, 2008], article 9 of the Convention is covered by articles 6000-ter, 600-quarter of the Italian criminal code. According to the definition furnished by article 600-ter a "minor" is a person under 18 years old. 600-quatre.1 defines the concept of virtual pornography but it does not cover explicitly article 9, par. 2 of the Convention concerning pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct. Article 9, par. 1 e) is covered by article 600-quarter c.p. that criminalizes the possession of child pornography. The Italian legislation goes beyond the aim of article 9 criminalizing also the organization of tourist rates with the aim to exploit the child pornography (article 600-quinquies).

# 3 PEER-TO-PEER AND FILE SHARING

People have always copied things: in the past most valuable items were physical objects, but today valuable things are increasingly less tangible, so they are just bits and bytes or can be accurately represented by bits and bytes.

A peer-to-peer (P2P) network is a distributed network architecture where the participants share a part of their own hardware or data resources (processing power, storage capacity, network link capacity, printers) [Schollmeier, 2001]. P2P applications are exploited in the fields of grid computing, distributed information infrastructure and above all file-sharing; file sharing programs are used in largely known for the extensive sharing of digital data, in particular copyrighted digital music and films. But they are emerging as a conduit for the sharing of pornographic images and videos, including child pornography. Most of the traffic in Internet is generated by P2P file-sharing applications [Sandvine, 2003].

Investigation on P2P networks is a case of data preservation which is for most countries an entirely new legal power or procedure in domestic law [COE, 2001]. It is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. First, because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. However, where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data. For legitimate businesses, a preservation order may also be less disruptive to its normal activities and reputation than the execution of a search and seizure of its premises. Second, computer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. These communications, as in the case of P2P, may contain illegal content, such as child pornography, computer viruses or other instructions that cause interference with data or the proper functioning of the computer system, or evidence of the commission of other crimes, such as drug trafficking or fraud. Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required. Third, where these communications contain illegal content or evidence of criminal activity and copies of such communications are retained by service providers, such as e-mail, the preservation of these communications is important in order to ensure that critical evidence is not lost. Obtaining copies of these past communications (e.g. stored e-mail that has been sent or received) can reveal evidence of criminality.

Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data.

## 3.1 Child Pornography in Peer-to-Peer Networks

P2P file sharing networks are considered a heaven of child pornographers. The anonymity and high file sharing speed of P2P file sharing networks allow them to share their collections in a quick and seemingly safer manner. Also if claims about the scale of criminal activity are more often based on

rumours rather than on verifiable empirical data [Walden, 2007], however P2P networks present an obvious environment for criminality and present investigators with unique issues in term of cyber-surveillance.

Nowadays, the practice of sharing file online is prevalent and there exists a number of ways to distribute digital files amongst a large number of online users. In the old days, file sharing may be done by establishing a file server on the Internet so that users could obtain a copy of the file by downloading it from the server [Law, 2011]. The traditional technology that supports file download is known as File Transfer Protocol. However, this sort of data sharing and distribution is found to be inadequate to cope with the ever-increasing demand for bandwidth and big files, such as movie. Furthermore, there may be problem of Single Point of Failure which largely reduces the availability of the whole file sharing system; thus, P2P technology is developed to address the problems of traditional client-server file sharing architecture. In a P2P network, each computer can operate autonomously and share resources with other computers without the need of central servers. New P2P protocols can also enable a computer to upload its downloading data to other computers within the same network. P2P network comprises a rapidly growing portion of communications traffic over the Internet, commonly used for transferring content such as audio and video files, but also increasingly other service such us voice telephony. Based on the design or configuration of a particular P2P application, any computer which has downloaded a part or the whole file, can become an uploader of the downloaded data to other participating computers in the network. This distinctive feature not only solves the problems of centralization, but also escalates the overall scalability and flexibility of the network. Common P2P software applications include BitTorrent, uTorrent, Bitcomet, eDonkey, eMule, Kazaa and WinMX, etc, each differing significantly in the way they operate on a continuum reflecting the extent to which centralized resources are utilized in the service. P2P networks therefore allow large-size files to be distributed among peers within a short interval of time. Moreover, some P2P networks are basically networks of anonymity, without the need of knowing the uploading computers between participating computers. This rapid and decentralized mode of sharing and the level of anonymity have facilitated crimes, especially child pornography, in the cyber world.

Though there are challenges in the context of P2P investigation, the following traces may also exist for digital investigation: the IP address of the peers who were uploading or downloading the digital resource online; the percentage of digital file copy that was owned by the peer; the software tool that had been utilized by peers to upload or download the digital resource; the index seed (e.g. Torrent environment) which was created by the uploader to share the resource; the storage location of shared resources at the sharer's computer.

P2P networks received widespread world attention during the dot.com boom, 1998-2000, not only for their utilization in illegal sharing of music files, most famously through applications such as the famous Napster service. In response, the music industry activated a series of legal allegations, around the world, aimed at shutting down similar services, as well as pursuing large-scale users, either through civil proceedings and through criminal copyright infringements trials.

The versatility of P2P networks, based around their decentralized structure, and their grater anonymity, has also inevitably attracted criminals, such as paedophiles and terrorists.

One mechanism for investigating P2P networks is for an investigator to infiltrate the network, establishing himself as a peer, node or a supernode, becoming part of the network with the specific objective of monitoring communication of illegal content, such as infringing a copyright material or pornographic data. Where such participation is carried out by a public law enforcement agency, it raises a number of legal issues, such as entrapment, incitement and the person's status. For a private investigator, the nature of the material being transferred and the investigator's role in its distribution raises obvious issues about illegal behaviour. However there are doubts about considering surveillance through participation as an act of interception: a broad range of traffic passes through the numerous computers linked to a P2P network; such traffic will constitute communications, the monitoring of which may be considered a form of interception, such as a search request for an MP3

music file held on one of the shared directories of the members of the P2P network. However, it could be argued that the person operating the node is an intended recipient of the communication, together with anyone else that is connected to the P2P network, even if they are not the final recipient, i.e. the person with the MP3 file. An issue for a court is whether the intention in this context is considered as meaning the final recipient, rather than the intermediaries in the communication process. Such an interpretation would be counter to the nature of how P2P networks operate, although it would perhaps be arguable were the sender able to show ignorance of this mode of operation, and therefore a reasonable expectation of privacy.
Tens of millions of people use peer-to-peer networks to share files: eMule and LimeWire are the most common file sharing software with hundred of million of users. Since there is no central server for the files, a P2P network is more advantageous if it makes up by many users; in addition, these software tools do not review or control the material in the network, so users can find any type of content: eMule and LimeWire cannot filter out certain illegal or objectionable content, but only users are responsible for the content that they place on or download from the network. Thus, file sharing software on peer-to-peer network are mainly used to exchange images or music, whether or not copyright protected, and child pornography.

Child pornography is a multi-billion dollar industry and among the fastest growing criminal segments on the Internet; producers try to avoid the prosecution by distributing their material across national borders; important scholars state that apart from widespread global efforts to suppress child pornography [Broadhurst, 2006] little progress outside of Europe may be expected in relation to the kinds of crimes covered by the Convention on Cybercrime.
According to TopTenReviews, in 2009, an estimate of more than four million websites contain pornography, i.e. about 12% of the total number of websites; the worldwide visitors to pornographic websites are more than 70 millions monthly; and pornographic downloads through P2P are about 35% of all downloads; in particular more than 100.000 websites offer child pornography.
Though the retrieval on keywords known to be associated with child pornography on Internet, United States General Accounting Office identified 1.286 titles or file names; of which:543 (about 42 percent) were associated with child pornography images; 34 percent were classified as adult pornography; the remaining 24 percent was non-pornographic material.
In another search, using only three keywords, 341 images are downloaded, of which 149 (about 44 percent) contained child pornography [Valadon, 2009].
A further Italian research, by in Arcobaleno 2011, on the presence of illicit material in Internet sites, discovered that: 97% of website are hosted in Europe and North America; in particular, USA was at the top of the table with 2267 websites, followed by Germany with 968 websites and Russia with 835; every day 135 website and 15 groups on social networks were born; 3.500 websites are financed by advertising banner; requests looking for child pornography on websites are from USA (more than 20%), Germany (17,6%) and other European countries.

### 3.2 Main Network Architectures

The eMule network is composed of several hundreds of eMule servers and millions of eMule clients: clients should connect to a server to getting network services [Kulbak, 2005]. Servers provide only a centralized indexing services (like in Napster): they don’t manage the file exchanged among peers.
Each eMule client is pre-configured with a list of servers and a list of shared files on its local file system. A client uses a single TCP connection to an eMule server for logging into the network, getting information about desired files and available clients. The eMule client also uses several hundreds of TCP connections to other clients which are used to upload and download files. Each eMule client maintains an upload queue for each of his shared files.
When a client highlight a file to download, he adds its name in the queue and advances gradually until he reaches the top of the queue, then he begins the download of the file. A client may

download the same file from several other eMule clients, getting different fragments from each of them.

The eDonkey 2000 file-sharing network is one of the most successful peer-to-peer file-sharing protocols. It is a hybrid peer-to-peer network with client applications running on the end-system that are connected to a distributed network of dedicated servers [Handurukande, 2006].
It has some specific differences compared with other protocols: contrary to the original Gnutella protocol [Ripeanu, 2001], it is not completely decentred; contrary to the original Napster protocol, it doesn't use a single server which is a single point of failure, but it uses a set of servers; contrary to KaZaa and the more recent Gnutella, it has no super-peer; eDonkey servers are slightly similar to the KaZaa super-nodes, but they execute a separate application, don't share any file and only manage information for the stability of the network.
In the eDonkey network, clients are the only nodes that share data while servers index their data. If a client wants to download a file (or a part of it), he has to connect to a server to get the necessary information about other clients offering that file; eDonkey protocol uses a MD4 hash to identify a file, independent of its filename. The implication for searching is that more steps are necessary before a file can be downloaded in the eDonkey network: user make a keyword search, the server answer the list of file that have the keyword in the filename; user requests which remote users have the file with a certain file-hash; finally, user connects to some of these remote user to download the file.

### 3.3 The Forensic Investigation Tools

The permeation of the criminal phenomenon through Internet requires new tools and methods to hinder it. On the other hand, Internet allows an effective contrast if it is supported by appropriate tools and expertises, aiding people called to investigate, make laws, judge, contrast child pimping and child abuse.
In order that contrast the phenomenon is really effective, we envisage that the transnational nature of Internet doesn't meet needs of local court systems and upsets the traditional survey systems. So operations of international cooperation among the various stakeholders involved are necessary to ensure that every local solution will not be inadequate to solve the problem that is configured a a global problem.
When it becomes necessary to investigate a crime of this type, there are two main issues: difficulty to identify the crime, such as the exchange of illegal material on peer-to-peer network; and difficulty to analyze data: when a person, starting from an Internet address, is supposed guilty of a crime, quite often investigators have to manage a huge quantity of seized materials.
Therefore investigators needs new strategies and software tools to support their tasks.
When it comes to online crimes, especially child pornography over the Internet, international cooperation is required because the Internet boundaries are vague, at best. Outlawing the traffic of such files in a given country is useless, since the files will remain readily available through the Internet on computers located in other nations.
Besides the example of internal collaboration and synergy, the international collaboration, through Interpol, was crucial in this fight against Internet child pornography and many other crimes.
There is still much to do, for instance, expand the software to support other file-sharing networks and become useful in other countries where different networks have become more popular.

For the analysis of activities in the P2P law enforcement field the main three tools in existence are: EspiaMule, FIVES and eMuleForensic. EspiaMule allows to find out, while data exchange is going on, if there are users who exchange files containing child pornography; FIVES performs data collection and analysis to extract the files containing child pornography after a computer has been identified, i.e. a post-mortem analysis approach; eMuleForensic extracts eMule log files in order to determine elements of awareness and to assess if there was been disclosing of that material.

EspiaMule, developed by the Brazilian Federal Police, aiming to make detections, utilizing the available expertise of its computer forensic examiners, using their tool SpyMule, a software application capable of monitoring the paedophilia file exchanges in P2P networks: the software works primarily as a spy agent, sweeping the World Wide Web in search of users sharing pornographic content files involving children or teenagers, although any other type of files could be searched as well. The Brazilian Federal Police developed this application for its investigations and evidence collection, allowing the gathering of information to subsidize large operations in the fight against Internet child pornography file sharing: this tool is based on the eDonkey network.

FIVES, a project funded by the European Union, brought partners from investigation agencies, academia and industry to work together to enhance the state of the art for tools available to law enforcement in the area of child sexual abuse investigation. It is a software which allows law enforcement organizations to handle efficiently large amounts of image and video material related to child sexual abuse. It allows police and law-enforcement agencies to: speed up the process of handling very large amounts of evidence material on seized computers, and separate previously known illegal material from new, potentially illegal, material by efficient file and file fragment matching; efficiently evaluate large amounts of new material by employing statistical optimization techniques. The aim are: to minimize the human effort needed when classifying new material; to improve the capability of linking new illegal images and video to previously known data by using object matching and image similarity detection techniques; to allow details of crime scenes to be linked between different image sets or videos. This facilitates the widening of investigations with the aim of rescuing the victims of sexual abuse.

The eMuleForensic system was designed and developed at the University of Bologna [Ferrazzano, 2011] as a tool to investigate and reconstruct the workflow of exchanges among peers; it is based on eMule, an open source software that allows to perform the activity of file sharing on P2P network based on the protocols eDonkey and Kademlia. In terms of forensic view, eMule does not save activities into log files; this is an unfavourable situation for the forensic examiner; nevertheless a useful source of information is a folder called *config*, where are stored a few files vital for the successful execution of the disk forensic analysis: in fact, in these files are stored full sets of information about the exchange activities through the application of eMule facilities and related to the user's configuration. Examples of these data are the *client-id* (a code for the identification of the client within the network of exchange) and the list of files offered for sharing with others. In binary file format lies the reason of the difficulty of reconstruction of the activities: they are not in easily readable or ordinary format (e.g. text or xml), and moreover the same data structure is coded only in the source code of eMule without any other documentation.
The four files, that are parsed by eMuleForensic to reconstruct the exchange activity that occurred on the system, are *AC_SearchString.dat, known.met, preference.dat, clients.met*.
The file called *AC_SearchStrings.dat* contains the last 30 keywords used in the internal engine of eMule as a search keys. This is a text file, then immediately readable, that allows to define and verify in clear what were the last researches carried out by the user: these data allow to understand what was the real interest of the user (e. g. searches for child pornography or just porn). The user, who wants to download a certain kind of file, types the keyword of interest and then gets a list of files whose names contain that keyword. Then, with a double-click, the user adds the selected file into the list of files awaiting download.
The file called *known.met* contains the list of the shared and downloaded material (and then it is automatically shared while it is in the shared folder) from the user. For each shared file, it is possible to find the hash value and a variable amount of tags used to describe any data of interest. The first byte indicates the version of the file (e. g. 0x0E or 0x0D). The following four bytes constitute an integer value that indicate the number of shared files by eMule. When this integer is greater then zero, information about that number of files is thus available. The file structure is

particularly complex because, for each shared file, a variable number of information is available. These data are treated with a tag system. The structure is not present in any source file, but it is recoverable through a reverse engineering from sever eMule source file, in particular *srchybrid/packets.cpp* that contains the implementation of the functions that allow reading and writing them. However, some tags are always present in this list, like hash file, size value and the filename.
The file called *preferences.dat* has the fixed size of 61 bytes: the bytes from the second to the seventeenth are interesting because they represent the user hash. The user hash, also known as user ID, is a string generated at the first run of eMule (or when the file *preferences.dat* does not exist). The sixth and the fifteenth byte of the user hash are always set respectively to the values 0x0E and 0x6F.The user hash may be omitted when the analysis focus is on a single system, but it becomes important when the analysis requires an assessment of the connections among nodes of the network: in such circumstances the only way to relate two nodes is to use the data that uniquely identifies each user on the network, i.e. the user hash. In the case of exchange of files between two users, say A and B, the user hash of A will be found inside the file called *clients.met* of the user B and vice versa. The file structure of *preferences.dat* is defined inside the source file called *srchybrid/preferences.h*.
The file called *clients.met* was conceived by the developers of eMule to implement the system of credits: where there are more clients queued to download a file, eMule adopts a criterion based on system of credits for the choice among the candidate remote receivers. This system gives priority to users who send larger amount of data, thus having to share many files; sending data is compensated and evaluated though a score. This information is maintained in the file *clients.met* saved on the computer of the uploader. The file keeps track of a number of user hash with other values, including how many data are sent and received.
We observe that if the forensic analysis is on a single computer then the case is generally simple and the files used for the analysis are *AC_SearchString.dat* and *known.met*: the former contains the keywords used by the user to search for illicit material on the network and it can be used to determine the awareness, while the latter contains the list of shared files, that is the list of files stored on the computer; it can be used to determine the amount of illicit files owned by the user.
If the computers involved are more than one, then the files *clients.met* and *preferences.dat* are used together with the previous ones. To evaluate if one of the user sends or receives data to or from another one a graph can be drawn that highlights the relationships among the various users under investigation. To analyze these file, eMuleForensic provides a Web interface that drives the investigator to find the searched information.

## 4 REFERENCES


[Broadhurst, 2006] Broadhurst R. (2006) Developments in the Global Law Enforcement of Cyber-crime, Policing and Police Strategies and Management, n. 29, pp. 408-433

[Clough, 2010] Clough J.(2010), Principles of cybercrime, Cambridge University Press

[COE, 2001] Council of Europe (2001) Convention on Cybercrime. Explanatory Report, at http://conventions.coe.int/treaty/en/reports/html/185.htm

[Ferrazzano, 2011] Ferrazzano M. (2011) Reati di pedopornografia in ambiente eMule: analisi dei log per ricostruire attività di scambio tra utenti, in Costabile G. and Attanasio A. (editors) IISFA Memberbook 2010, Experta

[Handurukande, 2006] Handurukande S. B., Kermarrec A.-M., Le Fessant F., Massouli L., and Patarin S. 2006. Peer sharing behaviour in the eDonkey network, and implications for the design of server-less file sharing systems, in Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems 2006 (EuroSys '06). ACM

[Kulbak, 2005] Kulbak Y. and Bickson D. 2005. eMule specification protocol, at http://www.cs.huji.ac.il/labs/danss/p2p/resources/emule.pdf

[Law, 2011] Law F. Y, et alii (2011) Digital Child Pornography: Offender or not Offender, in Martin M. V. (editor) Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives, IGI Global

[Picotti, 2008] Picotti L., and Salvadori I. (2008) National legislation implementing the Convention on Cybercrime, at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/ documents/ reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf

[Ripeanu, 2001] Ripeanu, M.. 2001. Peer-to-peer architecture case study: Gnutella network in Peer-to-Peer Computing, 2001 Proceedings of the First International Conference on Peer-to-Peer Computing (P2P '01). IEEE Computer Society

[Sandvine, 2003] Sandvine Incorporated. 2003. Regional Characteristics of P2P - File Sharing as a Multi-Application, Multinational Phenomenon, Sandvine

[Schollmeier, 2001] R. Schollmeier. 2001. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, in Proceedings of the First International Conference on Peer-to-Peer Computing (P2P '01). IEEE Computer Society

[Valadon, 2009] Valadon G., Magnien C., and Latapy M. (2009). Measurement of Paedophile Activities in eDonkey, in International Conference Advances in the Analysis of Online Paedophile Activity at antipaedo.lip6.fr/Proceedings.pdf

[Walden, 2004] Walden I. (2004) Harmonising Computer Crime Laws in Europe, European Journal of Crime, Criminal Law and Criminal Justice, vol. 12/4, pp. 321-336

[Walden, 2007] Walden I. (2007), Computer crimes and digital investigations, Oxford University Press

[Wall, 2009] Wall D.S. (2009) Crime and deviance in cyberspace, Ashgate