CROSSROADS OF INTELLECTUAL PROPERTY

INTERSECTION OF INTELLECTUAL PROPERTY AND OTHER FIELDS OF LAW

INTELLECTUAL PROPERTY IN THE 21ST CENTURY

CROSSROADS OF INTELLECTUAL PROPERTY

INTERSECTION OF INTELLECTUAL PROPERTY AND OTHER FIELDS OF LAW

ANA RAMALHO
AND
CHRISTINA ANGELOPOULOS
EDITORS

Nova Science Publishers, Inc.
New York

INTELLECTUAL PROPERTY IN THE 21ST CENTURY

Additional books in this series can be found on Nova's website under the Series tab.

Additional E-books in this series can be found on Nova's website under the E-books tab.

Library of Congress Cataloging-in-Publication Data

Ramalho, Ana.
Crossroads of intellectual property : intersection of intellectual property and other fields of law / Ana Ramalho and Christina Angelopoulos.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-61470-155-2 (hardcover : alk. paper) 1. Intellectual property. 2. License agreements. I. Angelopoulos, Christina. II. Title.
K1401.R34 2011
346.04'8--dc23

2011020241

Published by Nova Science Publishers, Inc. † New York

CONTENTS

In: Crossroads of Intellectual Property
Editors: A. Ramalho, C.Angelopoulos
ISBN: 978-1-61470-155-2

Chapter 3

THE CRIMINALIZATION OF OFFENCES AGAINST INTELLECTUAL PROPERTY RIGHTS – AN OVERVIEW OF THE EUROPEAN AND ITALIAN LEGAL FRAMEWORKS

Marco Grotto
Department of Scienze Giuridiche, University of Trento, Italy

1. INTRODUCTION

Copyright gives the author of an original work an exclusive right for a pre-defined period of time in relation to that work, with regard to its publication, distribution, and adaptation. How does the European Union respond to the problem of copyright violations? How does the Italian domestic legislation perform on the same issue? Is domestic legislation effective? And to what extent can copyright be protected at the detriment of other rights? This chapter attempts to answer these questions.

2. THE EUROPEAN LEGISLATIVE FRAMEWORK

For a long time, intellectual property rights were not foreseen by law, as traditional property rights were limited to the physical possession of material goods. The idea of 'copyright' developed in parallel to the increasing

importance acquired by the printed word. Copyright accordingly constitutes a set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. Copyright owners have the exclusive statutory right to exercise control over the copying and other exploitation of their works for a specific period of time.

At the European level, the European Union has aimed to ensure that adequate rules on the protection of intellectual property are applied in all Member States. In so doing, the Decision followed the basic obligations laid down by WIPO in its various conventions on intellectual property rights (such as the Paris Convention for the Protection of Industrial Property, the Berne Convention for the Protection of Literary and Artistic Works, the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, and the Washington Treaty in Respect of Integrated Circuits). The European Union possesses two important bodies to carry out this mission: the Office for Harmonization in the Internal Market (OHIM), which is responsible for the registration of Community trademarks, and designs, and the European Patent Office (EPO).

Among the European Directives that protect intellectual property rights, four pieces of legislation stand out. First, Council Directive 91/250/EEC of 14 May 1991 deals with the legal protection of computer programmes. Second, Council Directive 92/100/EEC of 19 November 1992 focuses on the rental right and lending right and on certain rights related to copyright in the field of intellectual property. Third, Directive 96/9/EC concerns database protection, and, finally, Directive 2001/29/EC of the European Parliament and of the Council adopted on 22 May 2001 (followed by Directive 2001/84 and 2004/48) deals with the harmonization of certain aspects of copyright and related rights in the information society. In what follows, I will concentrate on some of the above-mentioned EU Directives and I will expand on them listing the most recent pieces of EU law.

Directive 92/100 EEC is intended to bring about harmonized legal protection in respect of the rental right and lending right and of certain rights related to copyright in the field of intellectual property. According to the first paragraph of the preamble to the Directive, harmonization is intended to remove differences among national rules when those differences 'are sources of barriers to trade and distortions of competition which impede the achievement and proper functioning of the internal market'. The second recital states that 'such differences in legal protection could well become greater as Member States adopt new and different legislation or as national case-law interpreting such legislation develops differently'. For that reason, the third

recital states that 'such differences should therefore be eliminated in accordance with the objective of introducing an area without internal frontiers as set out in Article 8a of the Treaty so as to institute, pursuant to Article 3(f) of the Treaty, a system ensuring that competition in the common market is not distorted'.

In 1996, the European Union focused its attention on the protection of databases. Indeed Directive 96/9/EC of the European Parliament and the Council, adopted on 11 March 1996, aims at providing harmonized copyright protection for databases. It does not apply to the software used in the making or operation of the database or to the works and materials contained therein[1].

Directive 2001/29 reproduces and updates the principles and rules contained, *inter alia*, in Directive 92/100.

In 2004, Directive 2004/48/EC was adopted by the European Parliament and the Council. This deals with issues of enforcement of intellectual property rights, such as copyright and related rights, trademarks, designs and patents, The Directive, dubbed 'IPRED 1', and its corrigendum, 'IPRED 2',[2] requires all Member States to apply effective, dissuasive and proportionate remedies and penalties against those engaged in counterfeiting and piracy. In so doing, the ultimate objective is to create a level playing field for rights holders in the EU. As a result, all Member States are intended to have a similar set of measures, procedures and remedies available for rights holders to defend their intellectual property rights (be they copyright or related rights, trademarks, patents, designs, etc), if they are infringed. In particular, Article 3 of the Corrigendum to Directive 2004/48/EC provides that '1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive ... 2. Those measures, procedures and remedies shall also be *effective, proportionate and dissuasive* ...' Member States are strongly invited to introduce new criminal offences or amend the ones just introduced to ensure an adequate level of protection of intellectual property rights.

More recently, on 18 May 2005, the Commission adopted Recommendation 2005/737/EC that regulates collective cross-border management of copyright and related rights for legitimate online music services. Specifically, the Recommendation puts forward measures for improving the EU-wide licensing of copyright and related rights for legitimate online music services. This legislative update was necessary because of

[1]For this specific topic, see the Computer Programmes Directive.
[2]'IPRED' is an acronym of 'Intellectual Property Rights Enforcement Directive'.

problems associated with the new Internet-based services, such as 'web casting', 'streaming' and on-demand music downloads[3]. A summary of this kind of problem is provided in the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 16 July 2008 called 'An Industrial Property Rights Strategy for Europe'.

Finally, the most recent piece of legislation adopted at the EU level is represented by Directive 2009/24/EC of the European Parliament and of the Council, adopted on 23 April 2009. This Directive deals with the legal protection of computer programmes and requires that (Article 7) Member States provide, in accordance with their national legislation, appropriate remedies against: i) a person committing acts of putting into circulation a copy of a computer programme knowing, or having reason to believe, that it is an infringing copy; ii) the possession, for commercial purposes, of a copy of a computer programme knowing, or having reason to believe, that it is an infringing copy; iii) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer programme.

3. The Budapest Convention on Cybercrime

Another important legislative instrument related to copyright protection is represented by the Convention on cyber crime adopted by the Council of Europe on 8 November 2001[4]. With Decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. The EU Convention on cyber crime was the result of four years of intensive work on the part of this 'Committee of Experts on Crime and Cyberspace' ('Committee PC-CY'),

[3]Luder, T. (2007). The next ten years in E.U. Copyright: making markets work. Fordham Intell. Prop. Media and Ent. L.J., 1, 18.

[4]Garcia, O.M. (2004). La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime. In Picotti, L. (Ed.), Il diritto penale dell'informatica nell'epoca di internet, Padova: Cedam; Picotti, L. (2005). Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale. Diritto dell'Internet, 2, 189-204; Picotti, L. (2008). La ratifica della convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale. Diritto Penale e Processo, 6, 696-723; Sarzana di Sant'Ippolito, C. (2008). La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa. Diritto penale e processo, 12, 1562-1577.

which was entrusted by the Committee of Ministers with following up on previous Council of Europe recommendations on computer crime and criminal procedure problems linked with information technology. The Committee was given the particular task of preparing a legally binding treaty.

The Committee completed its work at the end of the year 2000 and worked in close coordination with the G-8 and other international bodies on the draft Convention on cyber crime. The European Committee on Crime Problems approved the final draft of the Convention in June 2001. The Committee of Ministers adopted the Convention on cyber crime in the occasion of the international conference held on 8 November 2001 in Budapest. Thirty States signed the Convention immediately, among which twenty-six Council of Europe Member States and four other countries that had participated to the drafting process (the United States, Canada, Japan and South Africa). The participation of the US at the Convention had especially important implications, as the US had introduced one of the earliest national laws specifically oriented around computer crime in the form of the Computer Fraud and Abuse Act – CFAA of 1984[5].

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

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

Several Member States, which had signed the treaty, experienced difficulty or delay in adapting domestic law to the requirements of the Convention. Italy is one of these States. Indeed, the domestic law that ratified the Convention was only approved in Italy in March 2008 (see below).

The treaty signed in Budapest on 23 November 2001 has received strong support from law-makers and practitioners throughout Europe and beyond, but has also been criticised on various grounds by a number of associations, particularly those active in the protection of freedom of expression[6]. That

[5]Yar, M. (2006). Cybercrime and society. London: Sage; Salvadori, I (2008a). L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking. Rivista italiana di diritto e procedura penale, 3, 1243-1285.

[6]Csonka, P. (2004). The Council fo Europe Convention on cyber-crime: a response to the challenge of th new age? In Ilarda, G. and Marullo, G. (Ed.), *Cybercrime: conferenza*

demonstrates that one of most difficult aspects of fighting cyber crime is the balancing of the prevention of crime with individual rights, such as privacy, freedom of speech.

The Convention on cyber crime pursues three aims[7]. The first aim is to lay down common definitions of certain criminal offences, which is very relevant to the harmonization of legislation at the national level. Following EU customary convention, Article 1 contains the definitions of 'computer system', 'computer data', 'service provider' and 'traffic data'. It should be noted that the Italian law of cyber crime Convention did not introduce the Council of Europe's definition in the domestic law system[8]. In doing this, the Convention aims at harmonizing domestic legal system by providing a common definition against existing diverse meanings across EU Member States' legal systems. The first part of the Convention concerns the introduction of harmonized criminal offences to the legislation of future contracting States, which could eliminate problems of dual criminality.

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

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

As concerns its structure, the Convention contains four chapters: i) Use of terms; ii) Measures to be taken at domestic level for substantive law and procedural law; iii) International cooperation; iv) Final clauses.

Specifically chapter i) (substantive law issues) covers both criminalization provisions and other connected provisions in the area of computer or computer-related crime. It first defines nine offences, grouped into 4 different

---

internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica, Milano: Giuffrè.

[7]Csonka, P. (2004). The Council fo Europe Convention on cyber-crime: a response to the challenge of th new age? In Ilarda, G. and Marullo, G. (Ed.), *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano: Giuffrè, 13.

[8]Guernelli, M. (2008). La legge di ratifica ed esecuzione della convenzione sul cybercrime: considerazioni sostanziali e processuali. *Rivista trimestrale di diritto penale dell'economia, 3*, 755.

categories, then deals with ancillary liability and sanctions. The Convention identifies the following offences: 'illegal access', 'illegal interception', 'data interference', 'system interference', 'misuse of devices', 'computer-related forgery', 'computer related fraud', 'offences related to child pornography' and 'offences related to copyright and neighboring rights'.

Copyright infringements are considered by Article 10 of the Cybercrime Convention. Such infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, for instance, are extremely frequent. Such protected works include literary, photographic, musical, audiovisual, and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks has made it necessary to include provisions on criminal law sanctions and improve international cooperation in this field. Each Party is obliged to criminalise infringements of copyright and related rights, arising from the international treaties listed in Article 10 (TRIPS and WIPO Copyright treaty), when such infringements have been committed by means of a computer system and on a commercial scale.

4. The Italian Legislation

The Italian system of copyright protection revolves around Law no. 633 adopted in 1941. Criminal offences are contemplated in Articles 171 to 181-bis. The most important rules are contained in Article 171- bis, which protects computer programmes and databases, Article 171-ter, which covers music and videos, and in Article 171, which deals with other behaviours against copyright.

The Italian criminal legislation involving copyright has been modified several times (see, for instance, Act no. 248/2000, Act no. 128/2004, Act no. 68/2003, Act no. 43/2005). The overlap between the different rules creates a system particularly difficult to manage[9].

[9]Morra M. (2008). I reati in materia di diritto d'autore. Milano: Giuffrè; Terracina D. (2006). La tutela penale del diritto d'autore e dei diritti connessi. Torino: Giappichelli; Terracina D. (2008). La storia infinita del bollino Siae. Diritto dell'Internet, 6, 598-602.

For instance, behaviours against informatics programmes and databases (Article 171-bis) and behaviours against music or video works (Article 171-ter) are punishable if committed with an intent of economic benefit. However, Article 171-ter refers to 'fine di lucro', which means that the offender aims at improving his/her economic situation. Article 171-bis, instead, refers to 'fine di profitto', meaning that it is sufficient that the offender avoids an expense. For instance, if a person copies a PC programme with the aim of buying only one copyright licence when he needs more, he can be convicted under Article 171-bis. Indeed, this would qualify as an expenditure saving. In contrast, if a person copies a song or a movie, he/she can be punished only if he/she makes a profit from such an activity[10].

As concern the P2P networks, the Italian legislator has attempted to limit the emergence of these networks by introducing a new penal sanction that addresses specific 'network behaviours'. For instance, Article 171.1.a-bis provides a fine from 51 to 2.065 Euros for those who make available to other persons a work protected by copyright by introducing the protected work into a network system with any type of IP connection. Article 171.2.a-bis imposes a penalty of imprisonment from one to four years and of a fine from 2.582 to 15.493 Euros on persons exhibiting behaviours which fall within the ambit of Article 171.1.a-bis, with the aim of improving their economic situation. Finally, Article 174-ter.1 provides an administrative sanction against those who illegally use, copy, or reproduce works protected by intellectual property rights – irrespective of the procedure through which the use, copy, and reproduction of copyrighted works has taken place (Di Amato, 2007; Flor, 2007).

In sum, Articles 171 (according to which the aim pursued by the offender does not play a role) and 171-ter (according to which the most serious penalty is a consequence of the aim of economic profit that the offender pursues) refer to 'upload operations'. Instead, Article 174-ter (which describes an administrative – not a criminal – offence) concerns 'download operations'.

However, this is a false dichotomy. Indeed, the modern P2P systems operate by splitting a single file into several parts. The software searches and copies the different part of the file the user is looking for by collecting them from different PCs. When the copy is completed, that is to say, when every single pack is copied, the software merges the different parts into a single file. In that way, every user makes available to the others not only a complete file,

[10]Gallus, G.B. (2008). Duplicazione a scopo di profitto del software e attività professionale. Diritto dell'Internet, 6, 576-582.

but also the single packs into which the file is divided. This means that when a single pack is downloaded (a behaviour that can be sanctioned in the administrative way), it is also made available to other users (a behaviour that is sanctioned by Article 171 or 171-ter as criminal offence). Hence, using software such as e-Mule, the user who simply intends to download a file risks being convicted also for uploading it! The only defence possible would involve *mens rea*: that is, the argument according to which the user did not know that the software worked in the way described above and did not intend to upload. Under these circumstances, the user cannot be convicted of the criminal offence.

Italy officially ratified the Cybercrime Convention with the Law no. 48/2008. The law revised some of the criminal offences that were already present in the Italian Penal Code, while also introducing some new offences[11]. Nevertheless, Law no. 48/2008 did not modify the existing Italian law on intellectual property right – that is to say, no modifications were adopted regarding the 1941 Law.

In the Italian legal system of intellectual property rights, a particular role is reserved for the *ad hoc* collective rights management body of the *Società Italiana Autori ed Editori* (SIAE), created under 1941 Law, which has protection, mediation and certification responsibilities. The Law also introduced the obligation to affix the SIAE distinctive sign on all media that contain an intellectual work. This is a peculiarity of the Italian legal system. Indeed, as mentioned in the Opinion of Advocate General in the Schwibbert case (see below), in the great majority of the European Union Member States, the law does not impose an obligation to affix the sign of the national body responsible for administering royalties relating to media. Only Portuguese and Romanian laws impose the obligation to affix such a label on reproductions, whether they have been imported or produced on national territory. The affixing of the label is regarded as a measure to protect copyrights against piracy. Greek and Cypriot legislators have contemplated similar measures, but have never adopted them.

Failure to affix the sign 'SIAE' results in the imposition of criminal penalties. Article 171-ter.1.c of 1941 Law, introduced by the Law no.

[11]Picotti, L. (2008). La ratifica della convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale. *Diritto Penale e Processo, 6*, 696-723; Grotto M. (2010). Council of Europe Convention on cyber crime and its ratification in the Italian legal system. *Sistema Penal and Violência – Revista Eletrônica da Faculdade de Direito – Programa de Pós-Graduação em Ciências Criminais – Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS, 2*, 1-17.

248/2000, provides: 'Any person who: ... sells or rents video cassettes, music cassettes or any other medium containing phonograms or videograms or cinematographic or audiovisual works or sequences of moving images which do not bear the mark of the Italian Society of Authors and Publishers (SIAE) in accordance with this law and with the implementing regulation ... shall be punished with a term of imprisonment of between three months and three years and with a fine of between ITL 500 000 and ITL 6 000 000.' This provision is justified on the ground that the SIAE sign is intended to inform consumers and the police that the reproductions of media are lawful. Similar provisions are provided for in the Article 171-bis.

5. Case Study No. 1: The 'Schwibbert' Case. Contrasts between European and Italian Legislation

The case-study can be summarized as follows. On 9 and 10 February 2000, the Italian Financial Investigation Unit ('Guardia di Finanza') discovered that Mr. Schwibbert, a resident in Italy and legal representative of the company K.J.W.S. Srl, held a certain number of CDs containing reproductions of the works of the painters Giorgio De Chirico and Mario Schifano. These CDs were available for sale at the company's warehouses. The CDs, which were imported from Germany, did not bear the distinctive 'SIAE' sign. On 12 February 2000, the Public Prosecutor (Procura della Repubblica) of the Criminal Court of Forlì (Italy) began proceedings against Mr. Schwibbert and charged him with having committed an offence under Article 171-ter.1.c of the 1941 Italian Copyright Law. Mr Schwibbert's lawyer called on the Italian Court to refer a question to the European Court of Justice (ECJ) for a preliminary ruling.

The problem submitted to the ECJ was worded in the following terms: 'Are the national provisions concerning the affixing of the SIAE marking compatible with Article 3 EC, Articles 23 EC to 27 EC, Articles 1, 8, 10 and 11 of Directive 98/34 and Directives 92/100 and 2001/29?'

As explained above, Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 lays down a procedure for the provision of information in the field of technical standards and regulations and of rules on

Information Society services[12]. This Directive was later complemented by three further Directives: Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998[13], Council Directive 92/100/EEC on rental right and lending right, and, finally, Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society.

Since the preliminary ruling was deemed admissible only in so far as it concerned the interpretation of the Directive 98/34, the problem was redefined as whether the obligation to affix the 'SIAE' sign applies to the CDs in question and, if so, at what point was that obligation was extended to such media. That is to say, to assess whether the SIAE marking was compatible with EU law it became necessary to assess whether the obligation to affix the SIAE marking was introduced before or after the notification to the EU. Indeed, EC Treaty provisions prohibit customs duties (such as the 'SIAE' sign) on imports and exports between Member States, as well as all charges with equivalent effect, unless they are notified to the European Union.

In sum, the referring Court asked whether Articles 1, 8, 10 and 11 of the Directive 98/34 preclude national provisions such as those at issue in the main proceedings, inasmuch as the latter provide for the initials of the Società Italiana degli Autori ed Editori (SIAE) to be affixed to media containing reproductions of intellectual works. Can the obligation to affix such initials be described as a 'technical regulation' within the meaning of the Directive 98/34? If so, it was necessary to check whether the draft technical regulation was notified to the Commission by the Italian authorities because, absent such a communication, it would have not been possible to proceed against Mr. Schwibbert?

Since observance of the obligation to notify is necessary for marketing those media products, the EU Court concluded that the sign 'SIAE' can be considered to be a 'technical regulation'. Under Article 8 of Directive 98/34, 'Member States shall immediately communicate to the Commission any draft technical regulation'. In consequence, in the event of non-compliance with that obligation, the technical regulation remains unenforceable against individuals.

Having specified the nature of the 'SIAE' sign, the next step was to ascertain whether Italy had fulfilled its obligations under Article 8. The 'Società Italiana degli Autori ed Editori' and the Italian Government claimed that the obligation to affix the distinctive 'SIAE' sign to media containing intellectual works was already applicable for *paper* media under the 1941 Law

[12]OJ 1998 L 204, 37.
[13]OJ 1998 L 217, 18.

a considerable period of time before the entry into force of the relevant Community directives. In addition, the SIAE and the Italian Government argued that the statutory amendments introduced in 1987 and in 1994, which extended the obligation to affix the SIAE sign to music cassettes and CDs, did no more than bring the legislation into line with technological progress, merely including new media within the scope of obligation to affix the SIAE sign. Accordingly, those statutory amendments did not have to be notified to the Commission.

Despite these arguments, the European Court rejected the Italian Government position, underlining that, according to the Directive 98/34, 'Member States shall communicate the draft again ... if they make changes to the draft that have the effect of significantly altering its scope ...'. The Court decided that the inclusion of new media, such as CDs, within the scope of the obligation to affix the distinctive sign 'SIAE' must be regarded as such a change. Indeed, the old Italian administrative regulation, adopted under the 1941 Law, only referred to paper media. By contrast, CDs are something significantly different from paper media. As a consequence, Italy would have had to notify the amendments adopted after the EU Directive entered into force. That change, however, has not yet been communicated.

The failure to observe the obligation to notify constitutes a procedural defect in the adoption of the technical regulations concerned and renders those technical regulations inapplicable and therefore unenforceable against individuals. Individuals may rely on that inapplicability before the national Courts, which must decline to apply national technical regulations that have not been notified in accordance with the Directive 98/34[14].

Following the ruling of the European Court of Justice, the Italian Supreme Court ('Corte di Cassazione') adopted a number of judgments[15], refusing to apply the Italian rules found to be in violation of European legislation. Nevertheless, the sentences issued by the Italian Court changed over time. Soon after the Schwibbert decision, the Italian Supreme Court decided that the lack of sign 'SIAE' could not be sanctioned in itself, but could be interpreted as a 'circumstantial evidence' of the illegal duplication of material protected

[14]Solda-Kutzmann, D. (2007), Contrassegno SIAE, mancata notifica alla commissione e inapplicabbilità della regola tecnica nei confronti del singolo. Giurisprudenza italiana, 2665-2667; Balsamo, A. (2008). Contrassegno SIAE e violazione della legge sul diritto d'autore. Cassazione penale, 1605-1607.

[15]See, for instance: Corte di Cassazione, Criminal Section no. VII, March 6th 2008, n. 21579, which can be read in Diritto dell'internet, 2008, 591 ff.; Criminal Section no. III, February 12th 2008, n. 13816; Criminal Section no. III, June 24th 2008, n. 27764, which can be read in Diritto dell'internet, 2008, 596 ff.

by copyright law. This reading has been criticized by several scholars, who argue that the European decision was thereby formally respected, but substantially ignored. Later on, with the sentence of 6 March 2008, the Supreme Court reversed its case law, deciding that the lack of sign 'SIAE' cannot be considered as a circumstantial evidence and that unauthorized behaviours have to be demonstrated in a different way.

Finally, the Italian Court addressed another problem raised by the ECJ's preliminary ruling, that of its consequences for the persons already convicted under Article 171-ter.1.c of the 1941 Italian Copyright Law. Indeed, following the Schwibbert sentence, the behaviour described in this article cannot be considered criminal, meaning that persons convicted (and imprisoned) for similar offence before the Schwibbert case had to be released and the penal effects of the conviction be deleted[16].

Recently, and following the Schwibbert case, the Italian Government adopted a new regulation for the 'SIAE' sign – the Decree no. 31 adopted on 23 February 2009. However, the Decree no. 31 was strongly criticized by scholars.

Firstly, the Decree reintroduced the 'SIAE' sign to the Italian legal system, thus restoring the previous legal framework, contrary to the Schwibbert ruling.

Secondly, the final text of the Decree, adopted by the Government and officially published, is different from that notified to the European Commission. Finally, the adopted Decree seems to have a retroactive effect, as Article 1.2 provides that the material produced and signed in the respect of the Decree no. 338 adopted on 11 July 2001 can be legally circulated. That is to say, the material than can be distributed is that that follows the requirements of the Decree that the European Court declared irregular because of the lack of notification.

Today, the Italian situation can be summarized as follows. The legal system provides offences that concern the (lack of) the 'SIAE' sign. These offences will apply in the future because the new Government Decree was notified to the European Commission as prescribed by the EU Directives mentioned above. For the period before the adoption of the new Decree, criminal offences cannot be applied .

[16]Terracina D. (2008). La storia infinita del bollino Siae. Diritto dell'Internet, 6, 598-602; Voltan, F. (2009). Il contrassegno SIAE e I riflessi della sentenza Schwibbert in Italia. Il diritto industriale, 1, 93-96.

6. Case study No. 2: the 'Promusicae' and 'Peppermint' Cases. the Contrast between Privacy and Copyright

The fight against P2P technology has developed in four different ways. First, aggressive advertisements in cinemas or during TV programmes were multiplied. Second, there has been great improvement in Digital Rights Management (DRM) systems, which limit the free use of copyright-protected movies, programmes, songs etc. by private users and allow the copyright owner to control and manage their rights. Third, there has been an increase in judicial prosecutions against file sharing networks and file sharing software[17] Fourth, judicial prosecutions against the P2P networks users have come to be based on information collected and stored by monitoring the users' activities made on the net[18].

The second and the fourth developments identified above triggered a conflict between the right to intellectual property and the right to privacy. On one hand, the owner of intellectual property rights wants to control and manage his/her right through an intrusive control of private activities. Nevertheless, this has profound implications on the fundamental right of users to privacy. That is particularly the case in Spain, Portugal, Austria, the Netherlands, Germany and Greece, countries which contain privacy clauses in their Constitutions. Italian legislation also introduced the right to data protection as a general principle (Article 3 of the new "Data Protection Code" – Decree June 30th, 2003, n. 196), considering it to be a fundamental right established and guaranteed at the European level. On the other hand, the claim to privacy often hides violations of copyright law made with the intent of enjoying an intellectual product without legal limitations[19].

The conflict between copyright and privacy is well illustrated by the two following cases.

---

[17]Among some of the most well-known cases of judicial prosecutions against file sharing networks and file sharing software there are the cases of AandM records, Inc. v. Napster, Inc. 239 F.3d 1004 9th Cir. 2003 and MGM Studios, Inc v. Grokster, Ltd. 545 U.S. 913 (2005).

[18]Caso, R. (2007). Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint. Profili di diritto comparato. Diritto dell'Internet, 5, 465-471.

[19]Caso, R. (2007). Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint. Profili di diritto comparato. Diritto dell'Internet, 5, 465-471; Guarda, P. (2008). Data protection, information privacy, and security measures: an essay on the European and the Italian legal frameworks. Ciberspazione e diritto, 1, 65-92.

The first case involved a Spanish association and the European Court of Justice: Productores de Música de España (Promusicae) v. Telefónica de España SAU, Case C-275/06 ('Promusicae case').

The Spanish Court describes the case in the following terms. Promusicae is a Spanish non-profit organisation of producers and publishers of musical and audiovisual recordings. It applied to the Commercial Court no. 5 of Madrid ('Juzgado de lo Mercantil no. 5 de Madrid'), asking for measures against Telefónica, a commercial company whose activities include the provision of internet access services. Promusicae asked for Telefónica to be ordered to disclose the identities and physical addresses of certain persons whom it provided with internet access services, whose IP address and date and time of connection were known. The Advocate General explained in his opinion that an IP address is a numerical address format, comparable to a telephone number, which enables networked devices, such as web servers, e-mail servers or private computers to communicate with one another on the internet. When a page is retrieved, the address of the retrieving computer is communicated to the computer on which the page is stored. Static IP addresses may be assigned in order to connect private users to the internet. However, that is rather rare, since each access provider has only a limited number of addresses available. Consequently, in most cases, including this one, dynamic IP addresses are used, meaning that the access provider assigns its customers a different address every time they access the internet.

According to Promusicae, several Telefonica customers used the KaZaA file exchange programme (a P2P programme) to provide access to files on their personal computers containing phonograms in which the members of Promusicae held the exploitation rights. Promusicae claimed that the users of KaZaA were infringing intellectual property rights and its aim was to discover the addresses of the persons concerned, in order to be able to bring civil proceedings against them. In order to take action against P2P users, Promusicae claimed that the access provider Telefónica should have communicated to Promusicae which users were assigned the IP addresses identified by Promusicae at the times it specified. The phone company, indeed, is able to find out which connection was used in each case, since it retains, after the connection has ended, the details concerning to whom and when it assigned a particular IP address.

By order of 21 December 2005 the Juzgado de lo Mercantil ordered the preliminary measures requested by Promusicae. Telefónica appealed against that order. It objected that, pursuant to Article 12 of the 'Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico', it could in no

circumstances provide the Court with the information. The electronic communications operator or service provider is allowed to supply the information which it is required by law to retain only in connection with a criminal investigation or if it is necessary in order to protect public safety or if national security is involved.

Hence, from a legal point of view, the problem consisted of a conflict between different European Acts.

On one hand, Directive 95/46/EC and Directive 2002/58/EC protect personal data, while the disclosure of addresses and the registration of internet connections by the phone company may represent a violation of privacy rights. Indeed, the 2002 Directive provides that Member States must ensure the confidentiality of communications by means of a public communications network, publicly available electronic communications services, and of the related traffic data and must, *inter alia*, prohibit, in principle, the storage of that data by persons other than users, without the consent of the users concerned. Still, according to Article 15 of Directive 2000/31 – which deals with certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – 'Member States shall not impose a general obligation on providers … to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'.

On the other hand, under Article 8 of Directive 2001/29, 'Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights … The sanctions thus provided for shall be effective, proportionate and dissuasive'. This means that each Member State is invited to introduce or improve criminal offences. Still, Directive 2004/48 provides a legal protection for some measures, procedures and remedies useful to enforce intellectual property rights.

It bears noting, however, that the Directive 2004/48 also states that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, in some cases, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services be provided by the infringer of copyrights.

In light of the above provisions, the Juzgado de lo Mercantil no. 5 de Madrid decided to refer the following question to the Court: 'Does Community law … permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus

excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?' As already noted, the Spanish reference for a preliminary ruling raised the question of how to reconcile the requirements of the protection of fundamental rights, namely the right to respect for private life, on the one hand, and the rights to protection of property and to an effective remedy, on the other. The EU Court's opinion was that the Directives 2000/31, 2001/29, 2004/48 and 2002/58 did *not* require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of *civil proceedings*. However, Member States, when transposing European directives, are invited to strike a fair balance between the various fundamental rights protected by the Community legal order. The second case that can be of help in illustrating the conflict between copyright and privacy protection is known as 'Peppermint case'. A Swiss informatics society, called Logistep AG, was instructed by a German record society, called Peppermint Jam Records GmbH, owner of intellectual property right on a long list of songs exchanged via P2P technology, to monitor Italian P2P activity and to store the IP addresses of people who uploaded or downloaded songs protected by copyright. As was the case in Spain, also in Italy only the civil Courts were involved. The story of the Peppermint case can be divided into three stages. During the first stage, the Civil Court of Rome ordered the phone companies to investigate the correspondence between IP addresses and the physical addresses of the consumer[20]. Using those addresses, the Peppermint lawyer sent hundreds letters to individual internet users inviting them to pay 330 Euros to avoid civil and criminal prosecution. During the second stage, the civil court rejected Peppermint's request[21]. Finally, the Independent Authority for personal data protection adopted a resolution on 28 February 2008. In that resolution, the Authority stressed that the data collecting made by Logistep constituted a privacy violation. Indeed, the personal data were collected and

[20]Civil Court of Rome, sentence February 9th 2007 can be read in Diritto dell'internet, 2007, 461 and Order August 19th 2006 can be read in Diritto industriale, 2007, 592.

[21]Civil Court of Rome, sentence November 22nd 2007 can be read in Il foro italiano, 2008, I, 1329; Sentence July 16th 2007, can be read in Diritto industriale, 2007, 585; Sentence July 14th 2007 can be read in Diritto dell'internet, 2007, 461, 588 and sentence November 27th 2006, not published.

stored for a private use (the collecting of data can be made only for a public purpose, like criminal investigations) without the consent of their holders. Hence, Peppermint had violated Article 122 of the Italian data protection Act (Decree no. 196/2003) and Article 5 of the European Directive 2002/58/CE, which provides that Member States 'shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so'. According to the same Directive, Member States have also to 'ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller'[22].

7. New Trends in Europe

In the last two years, important developments have occurred in the field of intellectual property right, as exemplified in the following two cases.

The first case concerns the action taken against the Swedish web site 'The Pirate Bay'. As is probably widely known, this website indexes and tracks BitTorrent (.torrent) files. It defines itself as 'the world's largest BitTorrent tracker' and is ranked as the 106th most popular website by Alexa Internet. The Pirate Bay has been involved in a number of lawsuits, both as the plaintiff and as the defendant. On 17 April 2009, Peter Sunde, Fredrik Neij, Gottfrid Svartholm and Carl Lundström, the website administrators, were found guilty of assistance to copyright infringement and sentenced to one year in prison and the payment of a fine of 30 million SEK (approximately 2.684000 Euros), after a trial of nine days. The defendants have appealed against the verdict.

[22]Caso, R. (2007). Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint. Profili di diritto comparato. Diritto dell'Internet, 5, 465-471; Gambini M. (2009). Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete. Giurisprudenza italiana, 2, 509-514; Viola L. (2008). Internet e privacy: il Garante per la protezione dei dati personali ne spiega i confini nell'ambito del caso "Peppermint". Studium iuris, 12, 1432-1435.

The story of 'The Pirate Bay' also involved Italy[23]. On 10 August 2008, the Public Prosecutor of Bergamo ('Procura della Repubblica di Bergamo') asked the judge to order Italian providers to block access to the website. At first, the injunction was granted by the Italian judge. Nevertheless, the lawyers for the 'The Pirate Bay' appealed and obtained a less strict sentence[24]. At the end of July, the Italian music industry federation FIMI (Federazione dell'Industria Musicale Italiana) claimed a refund from the Swedish website of 1.000.000 Euros. FIMI observed that 'The Pirate Bay' earned money selling advertisement spaces on its web site. FIMI thinks the money earned by the website in that way has to be returned to the authors who own the intellectual property right on the works illegal shared with the bit torrent files.'

The second case relates to the developments that have taken place in France[25]. The 'French philosophy' in facing piracy is, indeed, another example that helps explain the most recent legal trends in the copyright protection. Indeed, the French president has recently strongly attacked the problem of the pirating of songs and films, particularly over the internet. On 13 May 2009 the French Parliament approved Law no. 669/2009 entitled 'Loi Création et Internet' and currently called 'Hadopi' after the acronym of the enforcement agency it establishes ('Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet'). The law relies on online surveillance by copyright owners, usually film and music companies. The mandate was to ensure that internet subscribers "screen their internet connections in order to prevent the exchange of copyrighted material without prior agreement from the copyright holders" (Art. L. 336-3 of the bill). When record companies and film producers notice the works they own being pirated, they can report the IP address of the offending computer to the anti-piracy Agency. The illegal user is then required to install spyware on to his computer that will alert the Agency as to further infractions. A second alert brings a warning. Two alerts bring a ban from the internet of up to a year. In the original version of the law that meant that a government commission (rather than a Court) would have had the power to disconnect internet users who can be qualified ad 'repeated copyright offenders'.

---

[23]Sorgato A. (2008). The pirate bay: la fase cautelare (Nota a T. Bergamo, 3 ottobre 2008 e G.i.p. T. Bergamo, 1 agosto 2008). Il Merito, 12, 113; Angelopoulos, C.J. (2009). Filtering the Internet for Copyrighted Content in Europe. IRIS plus (Supplement to IRIS – Legal Observations of the European Audiovisual Observatory), 4.

[24]Available at: tinyurl.com/48j2ow.

[25]Fabbrini F. (2008). Francia: è arrivata l'ora dell'exception d'incostitutionnalité? *Quaderni costituzionali, 1*, 150-152.

However, some Members of Parliament requested that the French Constitutional Court assess that the new law from a constitutional perspective. On 10 June 2009, the Court said that the so-called Hadopi Law violated the principles of free speech and presumption of innocence. In light of the generalized use of the internet, the Court said that the right to freedom of expression implied the right to access the web. Thus, only a judge can decide if access should be denied. Finally, on 12 June 2009, the law was promulgated without the provisions declared unconstitutional by the Constitutional Court.

Following the developments at the European level (see below), the French Parliament discussed an amendment of the so-called Hadopi Law. In the new text, the 'three strike and you are out' policy is maintained, but the power to disconnect a user from the net is reserved not for the administrative Authority of the Hadopi, but for the Courts. As concerns the technical support, Extelia – a firm which operates in French mail services – will be entrusted with identifying, upon the request of music companies, the owner of IP addresses involved in illegal file sharing.

Setting aside specific case analysis, new developments concerning the protection of copyright can also be detected at the European level, paramount among these the so-called 'Telecom package' which amends the following Directives: Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services; Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities; and Directive 2002/20/EC on the authorization of electronic communications networks and services. The Telecoms Reform Package was presented to the European Parliament in Strasbourg on 13 November 2007. In April 2009, upon voting the so-called 'amendment 138', the European Parliament declared that no restriction may be imposed on the fundamental rights and freedoms of end users, without a prior ruling by the judicial authorities – in line with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information. After several amendments, the Telecoms Reform Package was passed into law on 24 November 2009 (see Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 and Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009).

The new Telecom law creates a new agency called Body of European Regulators of Electronic Communications (BERC) mandated to oversee telecom regulation in the Member States (see Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009). In addition, the new legislation allows Member States to set minimum quality

levels for network transmission services, thus partially implementing net neutrality. The EU law also allows Member States to disconnect internet users for illegally downloading copyrighted material, but only if there has been a prior, fair, and impartial procedure and effective and timely judicial review. The package entered into force in December 2009, after which Member States had 18 months to implement its provisions in national law.

The UK has also adopted a policy similar to the 'Sarkosy doctrine'. In October 2008, the action plan entitled 'Digital Britain – the future of communications' suggested the introduction of new 'technical devices' to protect intellectual property rights. Recently, the Parliament of the United Kingdom adopted the Digital Economy Act 2010, which regulates digital media and received Royal Assent on 8 April 2010 and came into force on 8 June 2010. According to the new legislation, the communications regulator (Ofcom) can impose obligations on Internet Service Providers (ISPs). The first obligation is that of sending notifications to subscribers accused of copyright infringements by rights holders. The second obligation is that of monitoring the number of notifications each subscriber is associated with. The ISP would then make this data available to rights holders on receipt of a court order. The UK legislation also established a mechanism whereby Ofcom would be granted reserve powers to oblige ISPs to utilize specified technical measures against repeat infringers, should these two obligations prove to be deficient in reducing infringement. In addition, the legislation ratains the possibility of adding, as a last resort, to the list of the so-called 'technical measures' the power to suspend a subscriber's account. Nevertheless, the proposal of forcing ISPs to suspend users' accounts has sparked reactions in the UK. ISPs and consumer groups, indeed, internationally consider the disconnection of users to be a disproportionate response.

In the Netherlands, in August 2009, the judge ordered the big BitTorrent indexer Mininova to clean up its site and remove all torrents that link to infringing content. BREIN ('Bescherming Rechten Entertainment Industrie Nederland', that is the 'Protection Rights Entertainment: Industry [of the] Netherlands'), clarified that its intention was not to shut the site down. Rather, the organization called for a filter based on infringing keywords and possibly digital fingerprints to be installed to guarantee that rights holders have sufficient means to protect their content. The court agreed with BREIN's assessment that Mininova was not doing enough to protect the rights of copyright holders and ordered the site to remove all torrent files that link to infringing content within three months or pay a penalty of 1000 Euro per infringing torrent with a maximum of 5 million Euro. The court did not agree

with Mininova's defense that it is impossible to moderate all torrents that are uploaded to the site. It further stated that Mininova encouraged its users to download copyrighted material, helped by several moderators that the site had in place. Mininova decided not to appellate the decision, which has to be done within three months.

Meanwhile in Italy, the debate on copyright protection is lively. One of the main problems regards the opportunity to sanction the final downloader by disconnecting him/her from the internet. Indeed, this solution is technically possible, but is it efficient? Furthermore, in order to sanction web users, who illegally copy songs or movies, the cooperation of internet providers is essential. Only the internet provider has the skills and knowledge necessary to indentify and store users' IP addresses. The Italian internet providers association has strongly criticized the French doctrine.

Given this state of affairs and in order to take into account to the different concerns of consumers, web providers and copyright owners, the Italian Government established the Anti-piracy Committee, which started work on 14 January 2009. This Committee aims to fight piracy in a new way. Indeed, the mandate of the Committee is to suggest to the Government what legal instruments are required to combat the piracy phenomenon effectively. Following this mandate, the Committee will publish its activities on an online forum (http://antipirateria.governo.it), on which any member of the public may give his/her opinion. Still, the Committee has made clear that decisions will be taken only after the interested commercial categories are heard. In this connection, several meetings were arranged with audiovisual producers associations, with internet providers and phone companies, with the BSA (Business Software Alliance) that represents software houses, and with the Italian and European consumer associations (Altroconsumo and the Bureau Europèen des Consommateurs). At the time of writing, the Committee had not yet finished its work.

In Italy, several significant legislative developments took place during 2009. In particular, two new laws were presented to the Italian Parliament for approval. The first one (no. 2188, called 'Barbareschi') suggested the creation of new platforms for the free and legal exchange of informatics material. That is to say, the copyright owners shall be paid through advertisements published on these new platforms. The Barbareschi proposal also suggested strengthening the involvement of ISPs in the fight against piracy.

The second law presented to the Italian Parliament (no. 2195 of the Chamber of Deputies, called 'Carlucci') is staked on the premise of forbidding the uploading of any material if carried out in an anonymous way. Both

proposals no. 2188 and no. 2195, despite their differences, were strongly criticized by ISP associations. As this paper goes to the press, none of the two proposals has been approved.

Recently, Law no. 99/2009 amended the Decree no. 231/2001, which contains the Italian legislation on corporate crimes, modifying Article 25-bis and introducing the new Articles no. 25-bis.1 and no. 25-nonies. The last of these (Article no. 25-nonies) provides that a corporate can be convicted to pay a fine if somebody commits a copyright violation (see Articles no. 171, 171-bis, 171-ter, 171-septies and 171-octies of Law no. 633/1941) in its interest or which procures it an economic advantage. This means that, for example, a company can be part of a penal trial if its employee uses counterfeited software on firm PCs. Indeed, in this case, the worker will have violated Article 171-bis of Law no. 633/1941, while the firm will have received an economic advantage in not having to pay the regular license fee.

CONCLUSION

This chapter has shown that the protection of intellectual property rights has become an important item on the EU legislative agenda, as attested by the several legislations analyzed above. Two conclusions can be drawn from the analysis. First, ensuring copyright protection is a difficult problem that will unlikely be solved in the immediate future. Often, previously existent legislation must be updated to combat forms of piracy. Second, ensuring copyright protection is a problem that cannot be faced by the domestic legislations of single Member States: international cooperation is essential to fight a transnational phenomenon of this kind.

The Italian domestic legislation has been modified several times. The aim has been to protect copyright from new forms of attack, such as CD duplication. Unlicensed software selling, represented by P2P networks, has also entered into the Italian legislative agenda with the amendments introduced in 2004 and 2005.

Music companies and the software houses, on their part, have tried to react to the increasing use of P2P software by taking legal action against both private users and the website managers (as in the 'The Pirate Bay case'). The result has been the emergence of a strong conflict between intellectual property rights and the right to privacy. Finding the right balance between the two has generated a great debate both at the European level and the Member State level.

At the European level, the prevalent position is that intellectual property is indeed a right, but that other fundamental rights have to be respected as well (see, 'Telekom package' and amendment 138). Despite the EU position, several domestic legislators have tried to introduce new and deep forms of copyright protection, sanctioning the final users with expulsion from the web community (see, the French 'Hadopi Law') or strongly involving the ISPs in fighting piracy (see, the Italian law projects 'Carlucci' and 'Barbareschi').

In this atmosphere, a question remains unsolved: is criminal law an efficient instrument to protect copyright? In order to answer this question, two observations are in order. The first is that the criminal offence is established to react to a massive attack at intellectual property right but punishing single behaviours. The second observation is that the user does not perceive the violation of copyright (i.e. downloading of protected material using P2P networks) as a crime. Hence, several web users associations have promoted the abolishment of copyright, which is perceived as a strong limit to freedom of expression.

In the author's opinion, criminal sanctions must be used only as an *extrema ratio*. Indeed, as concerns copyright, the Italian legislation contains many offences, but the system suffers from a lack of effectiveness due to lack of prosecution. Besides, an effective enforcement of intellectual property rights is purchased at the cost of other fundamental rights – such as the right to privacy or the right to have free access to communication means. For these reasons, civil or administrative legal instruments are more useful in the fight against digital piracy than the use of criminal law. The latter, indeed, should be reserved for the most serious cases. Nevertheless, the ultimate solution to the effective protection of copyright lies in the creation of a collective consciousness about the damages caused by copyright violations.