

Intellectual Property, File-Sharing and Privacy: The Challenge Is On The Internet

By Luciano Daffarra

This article represents a synthetic work meant to help readers understand the main problems concerning the protection of intellectual works over the Internet. Far be it from exhausting all the aspects of this matter, nevertheless it aims to establish some “landmarks” that may possibly show some ways of achieving a better balance among all the interests at stake, so that the sacrifice of one or more relevant juridical values may be avoided.

Attention is first drawn to this subject from a judicial controversy that caused a sensation in Europe, the so-called “Peppermint Case” (from the German record company Peppermint Jam Records GmbH) that can be summed up as follows: a few hundred Italian citizens received a notice from Peppermint Jam Records’ attorneys to erase some music files, the economic exploitation rights of which were detained by Peppermint, and which had been shared and put at the public’s disposal through the Internet from their personal computers, thanks to the use of file-sharing programs.

Peppermint was able to monitor and to ascertain all the infringements that had been committed online by such users, through the employment of a Swiss company, Logistep AG, which identified the IP addresses (i.e. the codes made up of a string of numbers that identify all the computers connected to the Internet) of the users that had made a massive file exchange activity of music works protected by copyright, without the consent from right holders.

The same record company, thanks to the data collected by Logistep, filed several injunctions at the Intellectual Property Section of the Court of Rome (under Art. 156-bis of the Italian Copyright Law), obtaining at first a discovery order towards the ISPs (Internet Service Providers) that were requested to disclose to Peppermint Jam Records the personal data of the users who had made massive online exchanges of works, the rights of which were detained by that company.

In a later moment, some of the magistrates of the Intellectual Property Section of the Court of Rome, mainly due to the appearance in the trials of the Italian Data Protection Authority, recognized that the ISPs were not obliged to disclose the names of their Internet connection subscribers, since that would mean disclosing the users’ personal data which were

protected by domestic and EEC laws on privacy. According to the judges, the monitoring activities carried out by Logistep on the Web might also be considered as an infringement of the same provisions and would be prohibited by law, too.

In short, the above legal case generated the problems that currently do not concern only Europe and the United States but the entire World. The litigation opposing the German record company to several private users and public institutions (the Data Privacy Authority in particular) brought forward a question that can be summed up as follows: *“Is file-sharing of protected intellectual work, made available without the consent of the right holders, impervious to IP protection rights due to privacy laws?”*

This question arose in Italy after the Peppermint case but its scope and extent corresponds to the pre-judicial question that the European Union Justice Court had to settle in C-275/06 lawsuit, opposing the Spanish Internet Service Provider Telefonica versus Promusicae¹ the Spanish music labels association, a topic that will be dealt with further in this paper.

In my view, any possible solution to this problem should not only be influenced by the existing legal system or by the various regulations concerning these or any similar matters, but it might derive from the choice of a mix of technological tools and juridical measures capable to supply useful elements in order to better understand the users’ and the right holders’ respective needs, with the smallest possible compression of primary rights involved in this unusual and complicated matter of interaction between inalienable values.

Let us try to be methodical now and see which are the main problems involved in these controversies.

1. Communication of Protected Works to the Public: General Rules and Effects

The distribution of digital contents by “communi-

1. <http://www.ipo.gov.uk/about/about-consult/about-ecj/about-ecj-refs/about-ecj-refs-2006.htm>—Request for prejudicial verdict in Case C-275/06 Juzgado de lo Mercantil n. 5 de Madrid dated June 26, 2005—Productores de Musica de Espana (Promusicae)/Telefonica de Espana S.A.U. in GUCE C 212/19 dated September 2, 2006.

cation to the public” mainly over the Internet, has called for the adoption of new rules on a European scale, that may establish and govern a brand new and peculiar copyright aspect in the information society, i.e. online copyright protection. Directive 2001/29/CE, the contents of which have been received by the Legislative Decree 68/2003 in Italy, dealt in *primis* with the implementation of such rules on a community scale. The technological innovations that are represented by online protected and non-protected contents on one hand and by the subsequent development of the so-called file-sharing programs on the other, certainly represent two historical events in recent communication to the public, because they have created a substantial change in the intellectual works distribution—according to Professor Jane C. Ginsburg of New York Columbia University.

In fact, in file-sharing, the distribution pyramid does not end with the consumer, as it happens for multimedia carriers, but it reaches the final user who becomes a “distributor” of copyrighted material transformed into digital format (files).

Even if there is no doubt that such opportunity represents a big step forward in the universal integration and globalization process that was generated by the use of communication instruments, the problem with the user’s role in such a context is that he does not always have a right over the goods that he retransmits through the Worldwide Web.

In my opinion, the new means of exploiting intellectual works, even in their fundamental role of knowledge exchange, are not enough to deeply change the system of rules that govern, control and protect them, nor are they to allow a wildcat development to the detriment of the right producers’ or right holders’ investments.

This belief, as far as the EU arena is concerned, is supported by the preliminary works and by the preamble of Directive 2001/29/CE concerning the harmonization of copyright in the information society, which gives useful information about the main points of rules governing the copyright in the digital world. Let us see which are the main points of the regulation at issue, as they are illustrated in Directive 2001/29/CE recitals:

(22) The objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works;

(25) The legal uncertainty regarding the nature and the level of protection of acts of on-demand transmission of copyright works and subject-matter protected

by related rights over networks should be overcome by providing for harmonized protection at Community level. It should be made clear that all right holders recognized by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterized by the fact that members of the public may access them from a place and at a time individually chosen by them;

(29) The question of exhaustion does not arise in the case of services and online services in particular. (... omissis ...);

(58) Member States should provide for effective sanctions and remedies for infringements of rights and obligations as set out in this Directive. They should take all the measures necessary to ensure that those sanc-

tions and remedies are applied. The sanctions thus provided for should be effective, proportionate and dissuasive and should include the possibility of seeking damages and/or injunctive relief and, where appropriate, of applying for seizure of infringing material;

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, right holders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States;

(60) The protection provided under this Directive should be without prejudice to national or Community legal provisions in other areas, such as industrial property, data protection, conditional access, access to public, documents and the rule of media exploitation chronology which may affect the protection of copyright or of related rights.

Art. 8(2) of Copyright Directive, whilst establishing that “Each Member State shall take the measures necessary to ensure that right holders whose interests are affected by an infringing activity carried out on its

■ Luciano Daffarra, Lawyer,
Daffarra d’Addio & Partners,
Milano, Italy
E-mail: luciano.daffarra@daffarrapartners.it

territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2)," has clearly pointed out which are the values at stake and how the access to any information that may be necessary in order to exercise such right should be allowed in the *acquis communautaire*, despite any surreptitious barriers.

As can be easily seen, the protection of intellectual property has been considered by the EC Legislator as an instrument aiming at strengthening the growth of knowledge, thus fostering investments in a field that has been deeply damaged by falsification crimes through the Web in these first years of the 21st century.

On the other hand, intellectual works that are at the disposal of millions of users who share them through file exchange networks and who run risks as for their personal security, their data protection and their personal property, have been recently subject to a tough test by several European Courts which have gone for a more than rigid application of provisions on "privacy protection" that actually anticipate a serious online protection of intellectual property.

2. Lawsuits Against Software Houses Producing Illegal File Exchange Programs

The heavy damage provoked by any infringement of copyright rules that occurs over the Internet at first made right-holders engage in lawsuits versus file-sharing software operators and distributors. Such content producers' reasons are simple, but not always well known.

In primis, it should be said that file-sharing systems are such that they allow the exchange of protected works and easily reach the users that want to share intellectual works. So, before attacking the users in order to prevent or to forestall any copyright infringement, right-holders have tried to prevent the proliferation of software allowing any illicit sharing of protected files.

That's why, in the years following the Napster sentence (2001)² music and motion-pictures producers engaged in several lawsuits that were aiming at eliminating the problem at the source, hitting the producers of exchange software whose illegal applications foster the sharing of protected files. U.S. RIAA (music) and MPAA (movie) companies were the leading promoters of these kind of initiatives.

2. <http://www.gseis.ucla.edu/iclp/napster.htm>.

The most important lawsuit concerning the legitimacy of some software programs that encouraged the illegal file-sharing of intellectual works and came to an end on June 2005, was that brought by the *U.S. Majors vs. Grokster Ltd. and Streamcast Networks Inc.*,³ two of the software houses that had developed some file-sharing programs (such as Morpheus and Kazaa).

After two conflicting decisions in first instance and second instance sentences,⁴ the US Supreme Court was unanimous in stigmatizing such companies' activity, that had put specific file-exchange software programs for protected works at the public's disposal. In fact, the judges ordained that the two file-sharing software distributors had wanted to make profit out of the copyright infringements by the users.

The Supreme Court then declared Grokster and Streamcast guilty of inducing users to infringe the copyright, thus giving them a vicarious responsibility in their infringements.

U.S. judges also established that *MGM vs. Grokster-Streamcast* lawsuit was substantially different from Sony/Universal lawsuit that generated the "Betamax" sentence.⁵ In fact, the Supreme Court pointed out that "*The Court of Appeal has read Sony's limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it. This view of Sony was error.*" In particular, judges defined the *software houses'* responsibility as a "vicarious" responsibility, because of the help that they had given the users in infringing the copyright (the so-called "*contributory infringement*") for which the American law provides for the simultaneous presence of the following conditions: a) direct infringement by the responsible subject; b) knowledge by the same of having committed an infringement; c) actual participation to the infringement by the subject who committed it.

Despite the significant impact of this decision over the whole sector of digital media and even if the companies involved in the Grokster lawsuit have stopped their activities, it was not possible to prevent other companies from developing and distributing file-exchange software programs, the structure of which has actually prevented any further action based on the Supreme Court juridical principles.

3. <http://www.copyright.gov/docs/mgm/index.html>.

4. <http://news.cnet.com/2100-1027-998363.html>; <http://www.policybandwidth.com/doc/20070227-JBand-Remand-Grokster.pdf>.

5. http://www.law.cornell.edu/copyright/cases/464_US_417.htm.

In the same way, the difficult market situation in the music sector caused by illegal file-sharing made the companies engage in specific lawsuits aiming at hitting heavy uploaders of massive quantities of files in order to make them give up such illegal activities.

3. European Rules on Copyright Civil Enforcement and Privacy Protection Measures on an International Scale.

The matters that I have dealt with in this article up to this point have allowed us to draw a portrait of the international (*rectius*: global) market where file-sharing takes place.

Now I shall examine the relationship between the EC Directives on copyright, civil enforcement and privacy protection, and outline the position of judges in some of the European Union countries about the problems at issue.

In the first paragraph of this work, I underlined the juridical reasons that justify a strong defense of intellectual works over the Internet and that require the adoption of proper measures in order to face online copyright infringements.

I am now going to see what the relationship is between EC rules on copyright enforcement as for the communication to the public of protected works and as far as privacy protection is concerned, and also briefly examine the text of Directive 2004/48/CE (the so-called Enforcement Directive⁶), that up to now I have indirectly quoted through references to Art.156-bis of the Italian Copyright Act about the “discovery right” that Peppermint Jam Records availed themselves of versus the Italian Internet service providers.

I shall then briefly examine the provisions of Directives 95/46/CE (Privacy Framework Directive), 2002/58/CE, 2006/24/EC on personal data processing, *data retention* and relevant circulation, a measure dated October 24th 1995, and compare them with the Enforcement Directive provisions.

With respect to the Enforcement Directive norms, what has been provided for by the relevant Article 8 (Discovery right) has not been weakened by Directive 95/46/Ce provisions in any way because:

a) In this provision there is a specific reference to information that can be discovered. It includes the judicial request of name and address. (...) of

producers, makers, suppliers as well as those of other previous product or service suppliers;

b) Art. 8.3 letter b) of the same Directive makes a specific reference to provisions that rule the use of any information to be enforced in “civil or criminal proceedings;”

c) As per Art. 6 of Directive 95/46/CE⁷ the name and the address of a telecommunication network subscriber are not to be considered as protected “traffic data;”

d) What provided for in letter c) above, actually makes the provision of Art. 8 letter e) applicable in this case, since such provision allows the treatment of any personal data that are necessary in order “to create, exercise or defend a right through available proceedings;”

Furthermore, the Privacy Framework Directive itself provides at Art. 15.2(b), that legitimate interest including “intellectual property and in particular copyright (...) should prevail over the privacy right-in case of automatized

7. On this point, the interpretation that has been given to this rule is based on Article 6 of the Privacy Communication Directive, that obliges all telecommunication operators to erase and to anonymize the data at issue, except for some invoicing data (Art. 6.2), in order to offer extra services to subscribers with their consent (Art. 6.3) and for the purposes as per Art. 15. The same directive provides for a definition of traffic data as per Art. 2(b) as follows : “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.” Recital 15 “Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.” In other words, traffic data are just technical data that are used to transmit telecommunications. They do not disclose any personal data to right holders who, otherwise, would not be obliged to ask for subscribers’ names, as we saw in Topware Interactive case. Obligations as per Communication Privacy Directive do not apply to personal data (like name and address) provided for by the Privacy Framework Directive. The Austrian Supreme Court sentence dated August 19th 2005 11 Os. 57/05z established that data supplied by ISPs according to a Judge’s sentence that obliges them to disclose the names of subscribers who carry out illegal activities on a telecom network are not “traffic data.” This sentence has been confirmed by the Vienna Court of second instance with a sentence dated April 12th 2007. On that occasion, the Court also stated that Art. 15 of the Privacy Framework Directive does not forbid to disclose the name of subjects involved in on-line infringements, which was made mandatory by the e-Commerce Directive. Please also refer to: <http://www.privacy.it/grupripareri200205.html>

6. This Directive originates from provisions of TRIPs (Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods) Trade dated April 15th 1995 (Marrakech) which rules this matter (see articles 41 to 50).

processing, as per provision 41 of the same Directive.”

Also Directive 2002/58/CE concerning the “*Personal data processing and privacy protection within electronic communication*” (the so-called Privacy Communication Directive) must be read in parallel with Art. 8(1) of the Enforcement Directive, that gives the Judicial Authority the responsibility of disclosing information concerning the origin and distribution networks of goods and services that infringe an intellectual property right (to any legitimate subjects that may require it) coming from the infringer (or from any third parties).

There are no doubts then about the existence of an indisputable⁸ “privacy right” belonging to private subjects, but it is true that the European Union rule making system is made in such a way that, much as the anonymity and privacy right may be deep rooted, the same is easily sacrificed when other primary rights deserve it, according to the general principles of law that find their origin in the thought of the German Enlightenment philosopher Immanuel Kant.

In this view, I want to underline that the Privacy Framework Directive shows in Art. 7 a series of cases where the personal data processing is however legitimate, and it allows Member States (Art. 13—Derogations and Limitations) to adopt some legislative measures as far as country defense, public security, etcetera are concerned. Such list of exceptions to privacy protection ends with the indication (in letter g) of “the protection of the concerned person’s or of other people’s rights or freedoms,” which surely includes the protection of intellectual property.

The reference to the “right for privacy” cannot therefore be used as a shield to intellectual property right infringements but, if anything, the “right to enforcement” and the “privacy protection” must be synergic goals that should never be considered as mutually subordinated. Even the sentence of the EU Court of Justice in *Promusicae* case expresses concepts that are in accordance with this principle.

On an international scale, despite Art. 12 of the Universal Declaration of Human Rights⁹ express a favor for global protection of the privacy right, there are several sentences of the Supreme Court and of other U.S. Tribunals that underlined in some cases a certain incompatibility between privacy right and freedom of thought guaranteed by the 1st Amendment to the American Constitution.¹⁰ The U.S. were

not the only ones to limit the possibility to turn to privacy protection when the infringement of any primary rights occurs.

In fact, within the European arena, while France for instance has provided for privacy right protection in its constitutional principles,¹¹ in the United Kingdom despite the existence of a law that recognizes privacy protection right, jurisprudence does not seem to protect the personal data consistently, thus weakening its application on the basis of Common Law principles.

We also need to underline that, as for the EEC set of rules, the recent approval of Directive 2006/24/EC¹² concerning the “Data retention in electronic communication services” and the previous provisions of the above mentioned Directives 2002/58/CE and 95/46/CE (besides the principles included in Directive 97/66/CE) have strongly strengthened the front of supporters of an absolute right for privacy protection, so much so that it has generated many of the problems discussed in the present article.

Within such a complicated set of rules that defend the need for a strong protection of intellectual property on one hand and then frustrate its reaching on the other hand, the relationship between Internet and Intellectual Property has actively occupied the magistrates of the single Countries of the European Union in a series of conflicting sentences about which will be discussed subsequently.

What makes this matter even more complicated and intricate is that, as far as privacy protection is concerned, the European Countries are represented, on an operational scale, by the “Art. 29 Data Protection Working Party” (DPWP), that was just created from Art. 29 of Directive 95/46/CE as an independent consultancy board of the European Commission for Data Privacy.¹³

Apparently, this Working Group has not kept a consistent line of action. An example of the progres-

8. Please refer to the article published on Harvard Law Review “The Right to Privacy” by S.D. Warren and L.D. Brandeis on December 15, 1995.

9. <http://boes.org/un/itahr-b.html>.

10. Please refer in particular to the *Bartricki vs. Hopper* sentence, 532 U.S. 514 (2001), Docket 99-1687.

In a stricter construction of New Hampshire Supreme Court: <http://www.courts.state.nh.us/supreme/opinions/2005/assoc145.htm>: the sentence referring to judicial data, extends its decision to cases concerning the companies’ financial data, with reference to a copious U.S. jurisprudence.

11. The right for privacy protection is implicit in the French Constitution of 1958 (Art. 34). Please refer to the *Décision* 94-352 of Conseil Constitutionnel dated January 18th 1995.

12. <http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf>.

13. DPWP’s tasks are shown in Art. 30 of Directive 95/46/CE and in Art. 14 of Directive 97/66/CE.

sive transformation of its opinions on privacy protection can be found in the analysis of some measures on privacy protection over the Internet. In fact, on January 18th 2005 the DPWP published the “*Working Document on data protection issues related to intellectual property rights*,” where you can read, among other things: “*b. Enforcement of copyright—While control and tracing is developing at the source with the intention of checking “a priori” every user downloading legally information on the Internet, the protection of copyright information also leads most of copyright actors to take actions “a posteriori” and to conduct investigations towards users suspected of infringements.*

Among the means used by right holders, the Working Party notes in particular the following: Peer-to-peer tools available on the Internet have been identified as a major mean to find information on individuals making available online, or downloading, protected information. The research conducted by right holders is usually based on the collection of the IP address of the users. This information is then combined with users’ data as detained by ISPs. In some cases the right holders directly request the identity of the user to the ISP in order to send cease and desist letters to the users. In other cases copyright holders request the collaboration of ISPs so that they themselves send letters to the users concerned asking them to take down the alleged infringing material, or that they disconnect users from the network.”

The Working Group statement goes on with an interesting note concerning right holders’ initiatives: “*The legitimate purpose followed by right holders to prevent misuse of protected information often results in the tracing of users and the monitoring of their preferences. In particular, the use of unique identifiers linked with the personal information collected leads to the processing of detailed personal data. Directive 95/46 on the protection of personal data provides for several principles that shall be complied with by any right holder in such case where personal data are being processed. Article 2(3) (a) of Directive 2004/48/EC, on the enforcement of intellectual property rights confirmed the principle that the Directive 2004/48/EC does not affect Directive 95/46 and therefore the application of the data protection principles.*”¹⁴

Whilst assessing the impact of right holders’ activi-

14. About this point, considerations as per paragraph 7 make one think that there is not a hierarchy in provisions protecting values that are equally sheltered in the Constitutional European Chart (Art. II-77).

ties, the DPWP recognizes the importance of monitoring over the Web, of course with proper care so as to respect privacy:

“The extent to which right holders obtain access to detailed users information varies depending on countries. In Belgium, right holders have been requesting the collaboration of ISPs to send warnings to users.

In the United States, ISPs were requested to communicate the ID of their clients directly to the music industry representatives, without Court order. This led to several court decisions (i.e., the Verizon case—December 2003¹⁵), where finally such direct communication of information to right holders was considered illegal by the Court.

As another example, the Australian legislation (through the “Anton Pillar order”) permits the search of inquiries, including domiciliary visits, by private actors such as holders of IP rights.

In order to connect alleged infringements with users responsible and to complete the profile of the user, attempt is made by right holders to use existing public registers, such as “Whois” databases, which keep personal details about those who have registered a domain name. It contains in particular information as to the name of the contact-point for the domain name, including phone number, e-mail address and other personal data. Some information is accessed directly online, while other details are kept off-line and must thus be requested to the controller of the database.

Finally, the Working Party notes that, considering the fact that the collection of personal information by right holders is regulated by data protection principles, discussions are taking place in several countries with stake holders in order to give them more flexibility as

15. A first important controversy in subjecta materia, concerned the U.S. evaluation about the Internet providers’ obligation or not to disclose the Web users that had made illegal file sharing through their own servers to any right holder that may ask for them. In the case at issue, telecom company Verizon versus RIAA, the former denied that there was an obligation to disclose the name of a “Web pirate” client because the laws in force in the U.S.A. (Art. 512(h) of DMCA), in Verizon’s opinion would only be binding if the service provided had kept a copy of such protected material infringement in its servers. As it is well known, such circumstance does not occur when file-sharing because there is no record of the exchanged works on the Internet provider’s files. With a sentence dated December 19th 2003, the Judges of District Court of Columbia decided that Internet providers’ obligations to disclose information about online infringements take place even if files are not physically present on their servers. Subsequently, such decision was cancelled because Verizon raised the problem of constitutional legitimacy. This situation has recently been overcome in the United States through the approval of PRO-IP Act (S 3325 dated January 3rd 2008).

to the processing of personal data. In this context, the French data protection legislation, for example, now includes an exemption aiming specifically at allowing the processing of judicial data by specific right holders defined by the law, in certain circumstances and subject to prior authorization by the French DPA.”

In this connection, it is easy to notice that the line of argument followed by DPWP, the Commission advisor as for data protection, is in favour of a copyright protection provided that it is made in accordance with Art. 6 letter c) of Directive 95/46 imposing that the use of data should be “proper,” “pertinent” and “not exceeding” in consideration of the purposes of their processing.¹⁶

More considerations about the DPWP are contained in several Position Papers, including the opinion of the Italian Privacy Guarantor of the day, that I think it right to hereby make reference to.¹⁷

Furthermore, the recent Art. 29 Data Protection Working Party position is opposite to the above described indications of Intellectual Property protection. In a letter sent on April 29, 2008, to the Commission for Justice and Freedom of the European Commission, Chairman Mr. Alex Turk and the President of WP on Police and Justice, Mr. Francesco Pizzetti, disclosed their commentaries to the presentation of the applicable measures on control and the Union border surveillance, which are the object of a project of rules that was disclosed by the EU Commission on February 13, 2008.¹⁸

Besides giving a definition of “search engine,” this document¹⁹ takes into exam some kind of data processed by such online search software programs

16. On this point it is interesting to quote the 2007 *Annual Report of the Personal Data Protection Guarantor* (pages 168 to 170) about WPDP’s work: “The document on technologies aiming at protecting the intellectual property (Digital Rights Management, DRM) contains some recommendations to national governments and to software producers about privacy. Such recommendations intend to underline the necessity not to use DRM technologies, so as not to limit the right to obtain information (because of unavailability of the original documents in which information is contained). Furthermore, the use of such technologies may involve some risks for privacy and for the safety of information systems, above all when they are used in a public environment; this involves the necessity to set up some DRM systems so as to keep the communication needs and the regulation bonds about data processing in a public environment in the due consideration.”

17. <http://www.privacy.it/garantenew20030618.html>.

http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/british_music_rights_en.pdf.

18. Art. 29 WP ref. WP 149 WPPJ ref: 02/2008.

19. WP 148 Adopted on April 4, 2008.

reaching the conclusion that the use of software aiming at identifying the IP’s address users is illegal. In particular, that report makes a previous reference to the Working Group (WP 136) that had established what follows: “... unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to **users that cannot be identified**, it will have to treat all IP information as personal data, to be on the safe side,” stating that such considerations should equally refer also to any operators who avail themselves of monitoring systems through search engines. In other words, if there is the possibility that the IP addresses may identify the physical subjects they correspond to, such data processing must have the concerned people’s consent.²⁰

The Privacy Guarantors’ indications in several European Union Countries, Italy included, and the above-mentioned measures of Article 29 Working Group do not seem to anticipate or properly take into consideration the sentence of the European Court of Justice about the Promusicae case, and don’t even recognize the necessity to stop the illegal file-exchange activities on the Web.

I would like to underline that another point about the relationship between privacy and copyright protection concerns the discrepancy between the sentence of EEC judges and the Advocate General’s position in her statement to judges in the Promusicae case. Advocate General Juliane Kokott concluded stating, among other things, that; “Consequently, the protection of the rights and freedoms of others under Article 13(1)(g) of Directive 95/46 cannot justify the communication of personal traffic data”²¹ contrary to what was stated by the Court of Justice in a sentence dated January 29, 2008.

In fact, paragraph 53 of the above-mentioned decision states: “It is clear, however, that Article 15(1) of Directive 2002/58 ends the list of the above exceptions with an express reference to Article 13 (1) of Directive 95/46. That provision also authorizes the Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary *inter alia* for the protec-

20. Par. 89 of her Conclusions dated July 18, 2007.

21. The following intervention of the Article 29 Working Party are all aligned to a strong defense of the privacy values and do not take into consideration the needs for a balance of same with IP protection issues. In this respect see Opinion I/2009 of February 10, 2009; Opinion 3/2009 of March 5, 2009; Working Document I/2009 of February 11, 2009. The full text is available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm.

tion of the rights and freedoms of others. As they do not specify the rights and freedoms concerned, those provisions of Article 15 (1) of Directive 2002/58 must be interpreted as expressing the Community legislature's intention not to exclude from their scope the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings."

The Court of Justice's conclusion in this circumstance is confirmed in the following paragraph 54 that states : *"The conclusion must therefore be that Directive 2002/58 does not preclude any possibility for the Member States of laying down an obligation to disclose personal data in the context of civil proceedings."*

As for the nature of IP addresses' "personal data" (or not) that the DPWP considers as guaranteed, even in this regard there are mixed positions within the European Countries. Let us recall some statements of the Court of Second Instance of Paris that exclude this possibility. For these decisions, which aim at respecting the personal nature of IP addresses, an appeal has been brought to the French Supreme Court and a sentence that should bring a little clarity on the nature of such identity data²² is expected shortly.

Considering that the European Community set of rules is very fluid and lacks bearings, France's recent choices with the signature of the "Accord en faveur du développement et de la protection des oeuvres culturelles sur les nouveaux réseaux," dated November 23, 2008, allow us to say that Europe in its entirety needs to find a proper solution to this problem, that may help avoid a clash with the involved institutions.

This agreement has been followed by the presentation of a bill introducing new criteria in fighting online infringements, in which Notice & Take-Down to users monitoring and communication tasks are at the public authority's charge, while right holders are vested with the task of finding new technological protection measures and of developing sifting technologies in cooperation with service providers.

The bill at issue (so called "Creation and Internet Law"), which has been examined by the National

22. Refers to the sentences of Court of Second Instance of Paris, on April 27th and May 15th respectively, about two actions brought by the French Photographic Producers' Association against two individuals, Mr. Anthony Guillemot and Henri Michel Marie Sebaux. In two different sentences, the Court decided that the use of programs aiming at collecting data that have been uploaded on the Web by the same users that infringed the copyright law, is not contrary to art. 2 of law dated January 6, 1978 (Intellectual Property Code).

Assembly²³ and that was recently stopped for its too severe sanctions against the Internet subscribers in the first vote of the French Parliament occurred on April 9, 2008, provides for the so-called three-strikes policy consisting in a gradual approach to online piracy. After the third infringement, only the Web users who keep on carrying out illegal activities despite being warned not to do so, will be deprived of Internet connection up to one year.²⁴

Under a different approach to the problem, i.e. the employment of technological measures for the purpose of preventing the illegal file-sharing of copyrighted works, I must underline that the decision of the Brussels Law Court of First Instance dated June 29, 2007 about the adoption of technical measures aiming at preventing online infringements²⁵ appears now to be in contrast with the DPWP's opinions on copyright protection, as reported before.

Despite the above, the action brought by the Belgian Authors Association, SABAM, with an injunction that was notified to Tiscali (now Scarlet) in order to prevent the library of their works from being exploited online through file-sharing, led to the issue of a preventing measure in favor of the plaintiff, and to the subsequent nomination of an expert (appointed by the judge) with the task of verifying if there were any technologically useful tools to prevent such online infringements and the cost of such applications.

On June 28, 2007, some days after the parties had been received by the judge, the Court passed its sentence. It stated that the expert had identified seven different technical acts that may prevent illegal file-sharing. Six out of these technological measures, concerned the control of online traffic and did not

23. The French Senate recently approved it with 297 favorable and 15 unfavorable votes.

24. In the United Kingdom, the competence to develop government initiatives against illegal file-sharing, is up to the BERR22 whose avowed goal, as per the signature of a Memorandum of Understanding dated July 24, 2008 between the British Government, right holders and service providers—is to "obtain a significant reduction of piracy through P2P in 2-3 years along with a change in the perception of and in the behaviour towards piracy. This is a serious problem involving the consumers on a large scale: we can only solve it if we succeed in changing the users' attitude on a large scale." In Italy on November 26th 2008, whilst voting rules about data retention, the Chamber of Deputies approved an agenda that, among other things, "engages the Government to provide for a proper balance between privacy and judicial protection of intellectual property rights within the digital environment."

25. <http://ip-watch.org/files/Sabam-2007%2006%2029-Jugt-Scarlet.pdf>

allow illegal contents to be blocked. The seventh one, called Copysense Network Appliance²⁶ and produced by Audible Magic, was deemed to be an effective tool to sift works that had been put at the public's disposal at a cost of 50 cents per month and per user to be paid by the ISPs.

The sentence at issue offers several hints, among which the Court's consideration according to which the sifting system does not involve any personal data processing, since it does not identify the Web users.

As for the juridical processing of IP addresses, the sentence of the Spanish Supreme Court dated May 9, 2008, is quite interesting: it stated that the same are not sheltered by the privacy protection right or by the confidential communication right. The Court made three fundamental considerations: a) there is a clear difference between a telephone call and a connection to the Web b) file-sharing or P2P users are undoubtedly aware that many of the data that they are uploading on the Web will become public and therefore available to every Internet user; c) the IP "string" does not identify a physical person but a PC. In view of these considerations, the Court declared that IP addresses are not personal data and therefore they are not protected by privacy.

Madrid's decision is not an isolated law episode within the European Union.²⁷ In fact, among the different decisions on this matter one must also recall *Brein vs. Chello*,²⁸ when on August 24th 2006 the Amsterdam Court ordered the service provider UPC (Commercial name: Chello) to disclose the names and addresses of their Internet service subscribers

that consistently carried out illegal online activities, among which there were the three major up-loaders of the Netherlands.²⁹

4. Conclusion

I have briefly examined some provisions and measures that are important to understand the complexity of questions concerning the relationship between intellectual property and privacy protection in the age of internet, both in Europe and overseas. In Europe the situation still seems to be fluid as for rules and jurisprudence on this matter but we can say that after the sentence of the Promusicae case we are on the way to finding a solution to the most important problems as far as illegal files on the Web are concerned.

Let's add that in the future the current deadlock will be overcome by government measures aiming at fostering a better relationship between ISPs, right holders and Web users. In this connection, the leading role of France with the soon-to-be approved three-strike-policy law leads us to hope that an easier path for all the European countries is near.³⁰

As far as the United States are concerned, the recent approval of PRO-IP Act should greatly limit the few obstacles caused by rules on personal data protection of those who use the Web to exchange protected files illegally.

In the months to come we shall better understand which direction will take this issue that nowadays concerns the information spread through the Internet Web all over the world. ■

26. <http://www.noncombatant.org/trove/audible-magic-copy-sense-sheet.pdf>

27. <http://www.goodwinprocter.com/~media/1DA7BD90AFE3499081379019EBA55E2E.aspx>

28. www.book9.nl/getobject.aspx?id=2777; <http://jilp.oxford-journals.org/cgi/content/abstract/2/6/402>

29. His decision overturned the previous decision (July 2005) of the same Court that raised privacy concerns resulting from the gathering of the data in the U.S.A. The more recent judgment establishes in principle that the interest of the rights-holders in tracing the infringers supersedes the privacy interest of the alleged infringers. The obligation of the ISP of providing the rights-holders with the subscribers data was previously stated by the Dutch Supreme Court in its decision of November 25, 2005 in the case Pessers-Lycos.

30. On December 5th 2008, the Swedish government said it is drafting a law that will allow record and film companies to pursue Internet users sharing music and movies illegally. The proposal makes it possible for industry lawyers to seek a court order to obtain the identity of a person behind an Internet subscription in cases of suspected copyright infringement. Companies can then seek damages from the file-sharers in court. Similar legislation exists in Finland, Denmark and several other European countries.