Intellectual property versus data protection on the internet

By Dimitra-Georgia Tsiaklagkanou

Introduction

Although intellectual property is all around us, sometimes we hardly realize it. A common example is the intellectual property of artists or performers, or the creators of computer programmes, which is easily accessible through the internet. Undoubtedly we live in an era when we can be informed through the world wide web about events happening around us, in the shortest possible time, at the lowest possible cost and in the convenience of our home. Most importantly, the internet may provide anonymity and freedom of movement by the user. However, despite the benefits of such freedom, the anonymity can result in abusive or non-compliant actions within the applicable legal framework. Although a detailed and thorough analysis of the issue may be impeded from differences arising from the laws of each country involved, there are common areas where the legal framework between countries colludes. Such common areas include, but are not limited to, the promotion of activities related to terrorism, drugs, and hacking (the most severe offences). Despite the severity of the cases previously described, intellectual property rights infringement is one of the most common offences committed through internet channels.

Although internet anonymity is assumed, the act of surfing the internet may leave a huge trail of personal data behind. The user may provide substantial information during activity on the internet; this leaves open the opportunity for a third party to extract data concerning the user's personal profile and preferences, for various underlying motives. The "assumed freedom" of internet usage creates an environment of false security so that the internet user feels comfortable about providing personal information.

Regarding the trail of internet usage contradiction thus arises. In this paper, we will attempt to analyze this contradiction from the perspective of intellectual property rights infringement. Can the creators of works and other rightholders use the identitification data of the internet users in order to be protected from the infringements performed by the latter? If yes, under what conditions? The result of balancing the protection of intellectual property and privacy is not obvious. For this reason, different jurisdictions have given different responses. In the present paper, we will consider this question under both Greek and French law. The choice of the first legal system is justified by the venue of this conference. The choice of the second is justified by the original solution given in the French legal system and the reactions to it at European level.

We will examine the processing of internet users' personal data and under which circumstances the data might be disclosed. Specifically, providers of electronic communication services may be required to reveal the personal data of their customers, that is to say internet users, under the applicable legal framework requirements, i.e. when an investigation by the authorities is taking place (I). An obligation thus arises to retain this data for a specified period of time, usually 1-2 years (II).

I. The obligation of electronic communication providers to provide the personal data of internet users

The need to identify the user, raises the question of whether the matching of his IP (Internet Protocol) address, with the identity of the subscriber to an internet access service, should be allowed (see section B below). In the above case, an issue arises of whether the IP address constitute personal data and can be considered among the information that the provider should store under certain conditions. Furthermore, we will examine whether it should be also covered by the definition of communication (see section A below).

A. The IP address as personal data and as part of communication

The IP address is automatically assigned by a provider of internet access services to any internet user. It is composed of four series of three numbers between 0 and 255 [Putman, 2011]. It can be static or dynamic, depending on whether it consists of the same series of numbers, each time a subscriber is connected to the internet.
The use of a dynamic IP address has no effect to the identification of a subscriber. The provider may obtain the identification information of the IP address holder at any time. It is possible to uniquely identify a subscriber connected to the internet on 25.05.2012 at 11:00, even if he was disconnected five minutes later. However, a shared IP address could be used by two persons living in the same house using the same internet access service. Further, if a subscriber leaves the network "open", other users may log in with the same address. Also, a hacker with only basic knowledge may steal an IP address of another user. Therefore, there is a possibility that the IP address cannot identify the internet user.
As described above, technically, the subscriber's identification is a possibility (see for a definition of personal data Directive 95/46/EC Article 2.a *"person is one who can be identified, directly or indirectly, in particular by reference to an identification number"*, Greek Law 2472/1997 Article 2.a, French Law 78-17 06.01.1978 Article 2.2; see for a definition of communication Directive 2002/58/EC Article 2). The question that arises, however, is whether matching the IP address to the identity data that a subscriber has given to his provider is also legally permitted, i.e. if the IP address is personal data or part of the communication, the use of this data should be carried out under the conditions and guarantees provided by each legal system. Otherwise, the user could be easily identified so that rightholders may initiate legal action against him to stop any infringement of intellectual property.

Under ***French law***, the qualification of the IP address as **personal data** seems quite perplexing. The Court of Appeal (*Cour d'appel*, CA) of Paris in its judgement of 15 May 2007, considered that the IP address does not constitute personal data information. Therefore, a specifically assigned official for this purpose (certified agent, *agent assermenté*) could identify a user participating in a file sharing network [Simon, 2009]. The court stated that the IP address ***"refers only to a machine and not to the person using it"*** (translation, "trans."). Similar statements are found in other decisions of that court, as of 27 April 2007, of 15 May 2007, of 12 December 2007, of 29 January 2008 [Pignatari, 2010; Szuskin, 2007; Caron, 2007].
By contrast, French courts decisions accepting the IP address as personal data, have also been issued (TGI Paris, 24.12.2007, CA Rennes, 22.05.2008) [Identification des utilisateurs de logiciels, 2008]. A judgement of 24 June 2009 states that *"an IP*

address is considered a personal data due to its correspondance with a number provided by an internet access provider, identifying a computer connected to the network … In view of the available technical means, ***this address appears to be the only evidence related to the person who posted the published content.*** *Even if the IP address can be spoofed using specially developed software tools, …this fact does not prive the IP address from being considered as data permitting to identify the content providers"* (trans.) [TGI Paris, 24.06.2009; Forest, 2011] .
The French Supreme Court (*Cour de cassation*), however, in its judgment of 13 January 2009 [Cass. crim., 13.01.2009] declined to resolve this issue in a final ruling. The Court merely stated that no processing of personal data has taken place in this case, since the *agents assermentés* had manually accessed a subscriber's list of musical files available through a file-sharing programme [Strugala, 2010; Chafiol-Chaumont / Bonnier, 2009]. It has been argued that *"if an authorization by the* ***CNIL*** (*Commission nationale de l'informatique et des libertés*) *is not required for a processing taking place not automatically, that may be explained by the fact that this processing does not concern personal data information"* (trans.) [Caron, 2009].

Given the fact that no clear response can be found within French legislation or case-law, we should look for other guidelines regarding the classification issue of the IP address as personal data information.
Article 29 Data Protection Working Party, in its **Opinion 4/2007** of 20 June 2007, states that *"while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual […]* ***on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user"*** [Article 29 Data Protection Working Party, 2007; Couland / Mariez, 2008]. This working group confirmed that *"IP addresses attributed to Internet users <u>are personal data</u>"* in its **Opinion 2/2002** "on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6", adopted on 30 May 2002 [Article 29 Data Protection Working Party, 2012].
Moreover, the **Decree of 5 March 2010** (*décret n° 2010-236 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet »*) classifies the IP address among personal data that the **HADOPI authority** (*Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet*, refer forward to p. 9) may process in order to send recommendations in cases of intellectual property infringement by internet users. Further, the ***Conseil Constitutionnel*** (**decision** no 2009-580, 10.06.2009) stated that *"the authorization given to individuals to collect data allowing to identify indirectly the subscriber to internet access services, results that those persons process personal data about infringements"* (trans.). The primary information collected for the identification of users is the IP address, and thus constitutes personal data.

A different approach to the above, can be found within the ***Greek legal system***. Here, the primary issue of concern is whether the IP address should be included within the definition of **communication**.
According to the **Prosecutor's Opinion 9/2009** [Prosecutor, 2009], the IP address is not protected by the principle of confidential communication provided by Article 19.1 of the Greek Constitution, since the communication via internet is *"<u>public communication</u>"* (trans.). *"As it is clear from the wording of Article 19,*

paragraph 1 (a), the confidentiality is protected for any means of communication, present or future, provided that these means of communication are by nature suitable for conducting communication within intimacy … . Therefore, there is such secrecy, i.e. in communication via fax, but not in communication via internet, since the latter is by definition public communication". "… confidentiality concerns the contents of the letter and, in general, of the responses and not the external communication data, i.e. the data of the sender or of the recipient. This means that disclosing the identity data of persons that make such abusive, threatening or extortionate phone calls is allowed … . In such cases, this does not constitute a violation of confidentiality, since there is no intention of the communicating persons to keep the conversation secret … " (trans.) (see also Prosecutors' Opinions 12/2009 and 9/2011).

However, considering communication via private messaging as public communication is open to criticism, i.e. the French case law has accepted that an employer **may not have access to messages marked as private correspondence**; a message may address a personal issue, as evidenced by the title of the message (CA Douai, 26.11.2004) [CA Douai, 2004]. The Supreme Court, has ruled, in an older judgement, that no access to employees' private messages is permitted to the employer, even if non-professional use of computers placed in the workplace is prohibited (Nikon, Cass. soc., 02.10.2001, Bull. V, n° 291; confirmed by judgement of Cass. soc., 12.10.2004, Bull. V, n° 245) [Mélin / Melison, 2007]. Moreover, as the Greek Data Protection Authority has pointed out on its website, *"The monitoring of employee's e-mail may be considered necessary only **in exceptional cases**. For instance, monitoring an employee's e-mail may be necessary to ensure confirmation or proof of certain actions on his behalf. These actions should include criminal activity and monitoring is essential to defending the legitimate interests of the employer. This occurs, for example, where the employer has legal responsibility for the actions of the employee"*.
Sending a personal message via the internet should not result in the waiving of the private nature of this communication, since the sender does not want third parties to peruse the message.
The increased risk of third party access to private communication has no influence in qualifying a message as private. This risk is due to the means of communication used, the facilitation it offers, the opportunities it provides and the risks that its use entails. Moreover, if we follow the same logic, we can argue that telephone communication by calls, or text messages via a mobile, cannot be considered as a private communication. On the contrary, **assuming the privacy of the communication via telephone, but denying that character in communication via internet, implies discrimination against the internet**, which is not justified under the principle of equality. Furthermore, this is not justified in terms of competition, since it provides a competitive advantage to a technological means of communication (the phone instead of the computer).
It has been also pointed out that even in communication through websites accessible to third parties (such as blogs), personal data not disclosed by users cannot be considered as part of public communication; users have taken adequate measures to prevent disclosure of such data [Sotiropoulos, 2009].

Moreover, the protection of the IP address as part of the communication should be accepted since at European level, a clear response is given to this question since 2002. The **Directive 2002/58/EC** specifies that *"a communication may include any naming, numbering or addressing information provided by … the user of a connection to carry*

out the communication" (paragraph 15 of the preamble to Directive 2002/58/CE). The same paragraph also provides that: *"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"* (see also the definition of the "communication", Article 2 (d) of the same directive).
Art. 4.1 of the **Law 3471/2006** transposes the Directive 2002/58/EC into Greek Law. Article 4.1. e (bb) of the Greek **Presidential Decree 47/2005** provides waiving of communication for specific data information, including the IP address (see also **Opinion of *ΑΔΑΕ* 1/2005**, refer forward to p. 6 second paragraph for the authority *ΑΔΑΕ*). Moreover, two judgements of the European Court of Human Rights, Judgement Malone v. United Kingdom (02.08.1984) and Judgement Copland v. United Kingdom (03.04.2007), found a violation of private life and correspondence (Article 8 of the European Convention of Human Rights, ECHR), due to the recording of phone numbers in the first and the monitoring of telephone calls, email and internet use in the second.

B. Matching a user's IP address with a subscriber to an internet connection

Should the IP address be considered as both personal data and part of the communication as described above, this data may be processed and disclosed by providers of electronic communication services to rightholders. This question was posed to the Court of Justice of the European Union in case *Promusicae* (Judgement of 29 January 2008, C-275/06) (1). In the Greek and French legal system, different responses were given; the French Law HADOPI (refer forward to p. 9) is of particular interest and should be presented (2).

1. The judgement Promusicae

As already mentionned above, in the case *Promusicae* the Court was asked to decide whether the service providers should disclose users' personal data to collecting societies. The Court replied that Community Law does **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"*. Instead, Community Law requires from Member states to interprete it so as to ensure *"a fair balance to be struck between the various fundamental rights protected by the Community legal order"*.
The Court confirmed this ruling, also in case *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* (Judgement of 19 February 2009, C-557/07) by stating that *"Community law …* ***does not preclude*** *Member States* ***from imposing an obligation to disclose*** *to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements. Community law nevertheless requires Member States to ensure that … they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights involved"* (see also judgement of 19 April 2012, *Bonnier Audio AB a.o. v Perfect Communication Sweden AB*, C-461/10).

2. Solutions provided by the Greek and French legal systems regarding intellectual property infringements committed through internet and, especially, the adventurous journey of the Law HADOPI in the French legal system

a. The waiving of confidentiality in the Greek and French legal systems

Under ***Greek law***, the waiving of confidentiality is not applicable for violations of the intellectual property. Article 19.1 of the Greek Constitution allows the waiving of confidentiality for reasons of national security or for offences of particular gravity (see also Law 3471/2006 Article 3). It is permitted for acts listed in Article 4 of Law 2225/1994. However, it has also been pointed out that a communication via file-sharing networks is not protected by Article 19.1 of the Greek Constitution since it is public, and non-confidential, communication [Prosecutor, 2009; Synodinou, 2010].

In Greek legislation, the Law 2251/1994 provides for the disclosure of the users' data either in case of felony offenses (Article 4) or for national security (Article 3). The **waiving of confidentiality** can be ordered by the prosecutor (Article 3.2) or the competent judicial council (Article 4.4). Only the competent prosecutor (Article 4.5) or a judicial authority or other political, military or police public authority, competent for an issue of national security requiring the waiving of confidentiality (Article 3.1), may submit such a request. The independent Hellenic Authority for Communication Security and Privacy (***ΑΔΑΕ***) verifies compliance with the provided conditions and procedure, that is to say Articles 3, 4 and 5 of the Law 2225/1994 and the Presidential Decree 47/2005 (Article 19.2 of the Greek Constitution, Article 1 of the Law 3115/2003). Furthermore, the waiving of confidentiality is provided by Article 253 A of Greek Code of Criminal Procedure for organized criminal activity under the requirements of the Law 2225/1994 [Tsolias, 2004].

The French Law 91-646 dated 10.07.1991 provides the **waiving of confidentiality** to protect the public interest, such as national security, the protection of important scientific and economic elements of France, the prevention of terrorism, crime and organized crime (Article 1 and 3). The Prime Minister, or a duly authorized person, can order the waiving of confidentiality (Article 4). They also should notify their decision to the National Control Commission for the security of interceptions (*Commission nationale des contrôle des interceptions de sécurité*) (Article 5). Thus, contrary to Greek Law, this administrative procedure does not require the judicial intervention. However, intellectual property is not included in the scope of this Law.
In addition, the waiving of confidentiality is allowed if a magistrate judge or a police officer investigates offenses punishable by more than two years imprisonment (*Code de procédure pénale* Article 100) [Dupuis, 2001]. Article L. 335-2 CPI provides for three years imprisonment for intellectual property infringements. Therefore, Article 100 of the *Code de procédure pénale* is applicable for these infringements.

It is worth mentioning that Article 15.1 of the Directive 2002/58/EC provides that *"Member States may adopt legislative measures **to restrict** the scope of the rights and obligations provided for in Article 5* (confidentiality of the communications), … *when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution*

of ***criminal offences or of unauthorised use of the electronic communication system*** *…"*.

b. Processing personal data in the Greek and French legal systems

Retaining and disclosing contact details also requires **processing personal data**; this processing should either be notified, or authorized, by the competent authorities (independent *Hellenic Data Protection Authority* "**ΑΠΔΠΧ**", *Commission nationale de l'informatique et des libertés* "**CNIL**"), depending on the nature of the data (simple or sensitive data) (Law 2472/1997 Articles 6 and 7; Law 78-17 06.01.1978 modified by the Law 2004-801 06.08.2004 Articles 23 and 25).
Article 5.2 (e) of the Greek Law 2472/1997 also allows the processing of personal data without the consent of the data subject concerned, when "*the processing is absolutely necessary so that the legitimate interests pursued by the controller, or the third party/parties to whom the data are provided, can be satisfied, and on condition that these interests are obviously superior to the rights and interests of the data subjects, and without compromising their* ***fundamental freedoms****"* (trans.). Nevertheless, this possibility is not provided by the Article 5.2 of the Law 3471/2006, which specifically regulates the personal data protection in the electronic communications.
Under French Law, the legitimate interests pursued by the controller or by the recipient should not disregard the interests or **fundamental rights and freedoms** of individuals (Law 78-17 Article 7.5). Therefore, disclosing personal data to third parties without the data subject's consent seems to be possible under these provisions since third parties' legitimate interests to protect their intellectual property rights could make the processing of personal data necessary.
However, even if Article 5.2 (e) is applicable under Greek law, the free and confidential communication should be considered as a fundamental freedom (i.e. Article 19 of the Greek Constitution) and thus the confidentiality should be waived only under the conditions described above (the Greek Law 2251/1994 and the French Law 91-646). By contrast, if the communication via file sharing networks is considered as public and non-confidential communication, the data processing could be possible following a notification to the Greek data protection authority or an authorization by the French data protection authority (refer forward to p. 8 second paragraph) [Synodinou, 2008].

It should be clarified that there is no overlapping of powers concerning the competent authority for the protection of personal data and the competent authority for the waiving of confidentiality (in the Greek legal system protection of confidentiality of free correspondence or **communication** under Article 19 paragraph 1 of the Constitution, protection of **personal data** under Article 9A of the Constitution, see also the Law 3471/2006 Article 13 for the competence of the two authorities regarding the electronic communications; in the French legal system, protection of communication confidentiality by the Law 91-646 dated 10.07.1991, protection of personal data by Articles 2 and 4 of the Declaration of the Rights of Man and of the Citizen) [Moritz, 2008]. Processing personal data is a broader concept than waiving confidentiality. Disclosing contact data requires both the processing of personal data and the waiving of confidentiality. By contrast, collecting personal data or retaining it requires the processing of personal data, but not the waiving of confidentiality [Papadopoulos, 2007].

The provisions of the Greek Law 2472/1997 are not applied to data processing carried out by the courts or prosecutors in order to investigate crimes punishable as felonies or misdemeanors if committed intentionally, crimes against property included. However, the provisions of Criminal and Procedure Law are applicable. Therefore, the Law concerning the waiving of confidentiality should be applied and thus processing personal data regarding intellectual property infringements is not allowed (Article 3.b).

Under French Law, processing of personal data relating to offenses, convictions and security measures can be carried out by the courts, public authorities or corporations managing a public service when acting within their legal powers, or the court officers in order to carry out the tasks entrusted to them by the law, or the collecting societies (Article 9 loi 78-17), in respect to other laws and namely the Law HADOPI (refer forward to p. 9). The collecting societies can process users' data if this processing is authorized by the CNIL. By contrast, the autorization by the CNIL is not required if the processing is carried out by the court officers (Article 25.3).

Directive 2004/48/EC (Article 8.1) provides that *"the competent **judicial authorities** may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided **by the … person** who: (c) was found **to be providing on a commercial scale services used in infringing activities**"* (Articles 63.2 of the Law 2121/1993 and L. 615-5-2 CPI). However, provisions that *"govern the protection of confidentiality of information sources or the processing of data"* should be respected (Directive Article 8.3).

Directive 2000/31/EC (Article 18) also provides for *"the rapid adoption of measures, **including interim measures**, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved"* (see Presidential Decree 131/2003 Article 17).

Further to the above, **Article 64 A** of the Greek Law provides that *"Rightholders **may request an order against intermediaries** whose services are used by a third party to infringe a copyright or related right"* (trans.). Article 65.1 of the Law provides that *"In case of infringement of copyright or related right, the author or the holder of related rights may demand **the recognition of his right**, **removing the offense and its omission in the future**"* (trans.) (see Articles 11 of Directive 2004/48 and Article L. 615-7 CPI).

Moreover, the Court of Justice of the EU, in case C-557/07 (as mentioned above), clarified that *"**access providers** which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether de iure or de facto, over the services which users make use of, must be regarded **as 'intermediaries'** within the meaning of Article 8(3) of Directive 2001/29"*. Thus "intermediaries" foreseen in Article 64A of the Greek Law can be also the access providers.

Pursuant to these provisions, the court can impose to a provider a filtering obligation regarding specific webpages infringing intellectual property rights [Kallinikou, 2010].

The first judgement of a Greek court was recently issued on 16.05.2012 (**Court of First Instance of Athens**, no 4658/2012) [Court of First Instance of Athens, 2012] imposing a filtering obligation to service providers. In this case, following a request of collecting societies, the court ordered the provider to take **technological measures** to make impossible the access of their subscribers to specific websites, when illegal presentation and exchange of works have taken place on these websites.

c. Application of the French Law HADOPI

In the ***French legal system***, there could be a recession of the protection of users' data information under certain conditions. The implementation of the system of "progressive notification" of a subscriber, the processing of personal data by an administrative authority, the authorization of this processing by the CNIL as well as the imposition of the penalty of interruption of internet access service by a judicial authority are considered as sufficient guarantees for the lawful processing of subscribers' data.

To be more analytical, the much-debated law HADOPI (see above to p. 3) imposes a duty of care to subscribers of an internet access service, so as to ensure that no acts infringing intellectual property take place through the use of their internet connection. The **Law HADOPI 1** (no 2009-669, *loi favorisant la diffusion et la protection de la création sur internet*, 12.06.2009) was passed after settlement by the General Assembly on 12 May 2009 and by the Senate on 13 May 2009. The law entered into force on 13 June 2009, without the provisions being criticized by the *Conseil Constitutionnel* in its decision 2009-580 (10.06.2009). This law was modified by the **Law HADOPI 2** (no 2009-1311, *relative à la protection pénale de la propriété littéraire et artistique sur internet*, 28.10.2009) issued after the decision of the *Conseil Constitutionnel* 2009-590 (22.10.2009). This law was also a subject of dispute between the presidential candidates in recent elections [Hollande, 2012; Frescaline, 2012).
This law provides for the HADOPI authority, competent to send letters to subscribers informing them of infringements of intellectual property. The HADOPI authority also recommends them to take safety measures, so that third parties do not repeat such acts by using their connection and warns them on penalties that may be imposed. In the case of repetitive violations, the authority may send a second letter within six months.
Thus HADOPI authority should process subscribers' personal data in order to send the above mentioned notices. This authority can retain technical data for as long as necessary, so as to exercise the powers conferred to it (Art. L. 331-28 of *Code de la Propriété Intellectuelle*, "CPI"). The processing of personal data is set forth by a decree issued by the *Conseil Constitutionnel*, after consultation with the CNIL (L. 331-29). The above decree was issued on 05.03.2010 (*Décret* n° 2010-236) and modified on 11.03.2011 (*Décret* n° 2011-264). The HADOPI authority also employs *agents assermentés* to collect the personal data of internet users (L. 331-21). These **certified agents** are appointed by the President of the HADOPI authority, under the conditions laid down by a decree of the *Conseil Constitutionnel*. They are subject to the obligation of professional secrecy (Art. L.331-22). The rightholders may also appoint *agents assermentés* authorized by the Minister of Culture to establish the infringement of intellectual property rights (L. 331-2), and then either contact the HADOPI authority or appeal to the courts (L. 335-2 to L. 335-4) [Benabou, 2009; Boubekeur, 2009]. It should be pointed out that the *agents assermentés* provided by Article L. 331-21 differ from the *agents assermentés* provided by Article L. 331-2, who are not approved by the Minister of Culture.

The matching of IP addresses of internet users to internet access service subscribers is carried out by the HADOPI authority. The identification data of the users after matching can be used only by the HADOPI authority or by a judicial authority. The rightholders or **collecting societies cannot have access to this data**. Moreover, the

CNIL must authorize in advance the processing of personal data (*autorisation*, Art. 25 *loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) [Gautron, 2009].
Should the subscriber not comply with the recommendations of the HADOPI authority, urgent court proceedings could take place after six months from the second letter sent by the HADOPI authority (L. 331-25 of CPI). The court can issue an order for interruption of internet access service, pursuant to Article 336-3. The initial provision that an independent administrative authority (HADOPI) could impose this penalty, was criticized by the *Conseil Constitutionnel*. Such a severe restriction on the fundamental right of freedom of expression, as depicted in the freedom of internet access, could not be imposed by an authority not providing the necessary guarantees as an independent admistrative authority, but only **by a judicial authority** (decision of the *Conseil Constitutionnel* 2009-580, 10.06.2009, §§ 15, 16).
The *Conseil Constitutionnel* had also, in its decision 2004-499 of 29 July 2004, demanded that the matching of the IP address to a user should be made by a judicial authority and only in the context of judicial proceedings (§ 13) [Colaud, 2009]. The *Conseil Constitutionnel*, in its decision 2009-580 of 10 June 2009 (§ 27), ruled that the processing of personal data by the HADOPI authority could only be carried out, if the data had been obtained with the intention of use by the rightholder in asking for judicial protection.
The ruling that the processing of personal data must be ordered by a court was also repeated by the *CNIL*, in its four Deliberations of 15 October 2005 (see Deliberation of the *Cnil* n° 2005-235, 18.10.2005). Thus, the CNIL refused four collecting societies (Société des Auteurs, Compositeurs et Editeurs de Musique "Sacem", Société civile des Producteurs Phonographiques "SCPP", Société civile des Producteurs de Phonogrammes en France "SPPF", Société pour l'administration du Droit de Reproduction Mécanique "SDRM") to process users' data. However, the *Conseil d'Etat*, in its decision of 23 May 2007, stated that this argument does not justify by itself the contested decisions (CE 23 mai 2007, n° 288149) [Drouard, 2007].

d. Criticisism against the Law HADOPI

The initial provision that the interruption of internet access service could be imposed by an independent authority had caused reactions at European level. In discussing the **Directive 2009/140/EC** amending Directive 2002/21/EC, the rapporteur deputy Guy Bono proposed the amendment 138/46, providing that the interruption of internet access service could only be imposed by a judicial authority. This amendment was passed by the Parliament, but not accepted by the Commission. At conciliation, before the Council of Ministers, a less binding version of a ***"prior, fair and impartial procedure"*** finally was adopted instead of judicial intervention. However, the principle of proportionality should be taken into account while imposing such a penalty, as a guarantee for the protection of fundamental rights. Specifically, according to Article 1.1.b of the Directive 2009/140/EC, restrictions to *"those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society"*.

However, the interruption of internet access service, even when ordered by a judicial authority, cannot be accepted without reservations. In the era of technology, the use of the internet is necessary not only for information but, also, for free expression of opinions, or exercise of a profession. For instance, a lawyer must search for case law

and articles online. The law expressly provides for consideration in these cases that subscription to the internet access service is conducted by a company or a professional (L. 335-7-2 al. 1). However, a professional does not work only at his office.
Furthermore, professionals should not be treated more favorably than individuals and hence giving the privilege of professional freedom over against the freedom of individual expression. The latter is also a fundamental human right and requires its weighting over the protection of intellectual property. Neverthless, the penalty of interruption of internet access service is not imposed in every case, but it remains at the discretion of the judge.

The Law HADOPI also introduced a **presumption of guilt** against the subscriber to internet access service (decision of the *Conseil constitutionnel* 2009-580, § 18) [Bitan, 2009]. The subscriber is assumed responsible for an act infringing intellectual property rights, committed through his internet connection. He may be relieved of liability by proving to have taken the necessary security measures to avoid such acts or by proving either third party's fraudulent conduct or force majeure. Therefore, all subscribers are considered responsible for acts committed through their internet connection, without having contributed in any way to these infringements of intellectual property [Gitton, 2008]. The exemption from their responsibility by reversing the presumption seems extremely difficult. They have to prove that a third party used deceptively their internet connection. It does not constitute adequate evidence that they are not themselves the offenders of intellectual property rights [Colaud, 2009].
However, the subscriber is **not liable for intellectual property infringements that a third person has committed** (as are parents for the actions of their minor children, Article 1384 of French civil code (*Code Civil*), Article 923 of Greek civil code). A person could be relieved of his liability if he proves that he has properly supervised (i.e. the usage of his internet connection) or that the injury could not be prevented (under Greek law), or that the parents could not prevent the event giving rise to liability (under French law). Thus, in the case under examination, a strict responsibility is not established due to the actions of a third person, but rather a **subjective liability** for failing to take security measures for their internet connection.
It should be explained that, under French law, a person liable to an obligation of result can be relieved only by proving that the result is due to some external event (*cause étrangère*) or force majeure [Colaud, 2009], but not by demonstrating no fault. In the present case, however, the subscriber may be relieved of his liability should he prove not only the presence of an external cause but also no fault. Thus, it seems that there is a **reinforced obligation of means** and not an obligation of result. [Heinich, 2011]. This responsibility can be compared to the false (*νόθο*) strict liability under Greek law.

It should also be noted, that the initial law HADOPI 1 provided for a penalty of interruption of internet access service only for the internet user whose internet connection was used for breaching intellectual property rights, and not for the person infringing these rights. The law HADOPI 2 extended the application of this penalty, also to the latter, in addition to other penalties that may be imposed to him, i.e. imprisonment, fines (provided by Articles L. 335-2, L. 335-3, L. 335-4 of CPI) [Chavent-Leclère, 2011].
Moreover, despite the neutrality of the used terms, the HADOPI law aims at suppressing file-sharing on networks (peer-to-peer), where there are also **other**

spreading techniques for reproduction of works, such as streaming, or file-sharing in closed networks [Fr. Macrez / J. Gossa, 2009]. It should be noted that the previous law on copyright and related rights of 01.08.2006 (*loi sur le droit d'auteur et les droits voisins*, DADVSI), was criticized by the *Conseil Constitutionnel*, in its decision 2006-540 (27.07.2006), for discriminating file-sharing networks to other forms of electronic communication though which intellectual property may be infringed. These comments were taken into account by the legislator, while adopting the law HADOPI (Thoumyre, 2006 ; Tafforeau, 2011].
Although the internet access service can be interrupted pursuant to an order of a court, the subscriber still has to pay the fee to the service provider. Thus, he pays **a charge not corresponding to a service**. However, there is no reason why the provider should take advantage of this amount; the latter did not prevent the intellectual property infringement. Indeed, two active persons on the internet are treated differently [Gitton, 2008]. On the one hand, the subscriber is responsible for intellectual property infringements not committed by himself. On the other hand, the service provider is relieved of his liability for these actions under Articles 12 and 15 of Directive 2000/31/EC (Articles 11 and 14 of Greek Presidential Decree 131/2003, Article 6 of the French Law 2004-575). Therefore, the individual subscriber is treated more severely than the professional provider (as well as than the professional subscriber as seen above, p. 11 first paragraph), while all the parties mentioned are unaware of the infringement of the intellectual property.
The principle of proportionality requires that the penalty should not be extended to telephone connection or cable TV services on the grounds that they are likely to be provided by the same provider [Colaud, 2009].

e. EDPS and Greek case-law regarding the "three strikes disconnection policies"

Further to above, the European Supervisor of Personal Data (**EDPS)** has pronounced upon the "**three strikes disconnection policies**" by considering that *"a three strikes Internet disconnection policy as currently known - involving certain elements of general application - constitutes a disproportionate measure and can therefore not be considered as a necessary measure"* (Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010/C 147/01) [EDPS, 2010].
The **Court of First Instance of Athens** (no 4658/2012) [Court of First Instance of Athens, 2012] is opposed to the interruption of internet access service. We deem it appropriate to quote part of this extremely interesting ruling: "*Technological interventions in the information society where the access service **providers interrupt** or degrade significantly services over their networks, which are based on p2p technology, so as to deprive internet users from accessing to these ... as a whole should be considered as **incompatible with Greek Law**, as contrary to Article 5a paragraph 2 of the Constitution, which establishes the right to participate in the information society, as applied in conjunction with Articles 5 § 1, 5 § 1, 14 § 1 and 16 § 1 of the Constitution and interpreted in accordance with Article 10 ECHR, Art. 19 § 2 of the International Covenant on Civil and Political Rights and Articles 11 and 36 of the Charter of Fundamental Rights of the European Union (with the restrictions of Article 52 § 3 of this Charter). The constitutional right includes, inter alia, the claim to have access to infrastructure of the information society ... Therefore, the p2p technologies (peer-to-peer) is part of this material and technical infrastructure of the information society ... These are the most advanced technologies*

for the time being, in order to transfer information in the internet, and are used for, among others, perfectly legitimate uses. As a concequence, degradation or interruption of access to these services, for the protection of intellectual property, would result in the suppression of such perfectly legitimate uses, and therefore, it would ***restrict more than necessary*** *the right to participate in the information society and other freedoms provided by the Constitution"* (p. 13 of the Judgement) (trans.).
In the United Kingdom, the Digital Economy Act 2010 provides a system of gradual notification of subscribers infringing intellectual property rights, following the example of the Law HADOPI. The copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright infringement. The interruption of the internet access service can be ordered by the Secretary of State and the right to an appeal process made before a court (a First-Tier Tribunal) is also available [Digital Economy Act 2010; Taylor, 2010]. In Germany, such legal framework does not exist [Szuskin, 2009]. Finally, in France, it seems that maintaining the solution of the "three strikes" system is no longer certain following the presidential elections on 6 May 2012.

II. Obligation to retain data

1. The Directive 2006/24/EC : data retention for security reasons

The providers of publicly available electronic communications services or of public communications networks should retain subscribers' personal data in order to disclose such data, if asked. The **Directive 2002/58/EC** provides for the retention of subscribers' or users' personal data for as long as necessary for the service charge (Directive Article 6.2, see also the Greek Law 3471/2006 Article 6.2). However, Article 15.1 of the Directive 2002/58/EC allows Member States to adopt legislative measures providing for the retention of data for a limited period justified on the grounds of prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.
The **Directive 2006/24/EC** provides for the retention of subscribers' or users' personal data for a period of 6 months to 2 years (Article 6). Providers are required to provide subscribers' personal data to the competent national authorities in specific cases and in accordance with national law (Directive 2006/24/EC Article 4).
This requirement was incorporated into Greek legislation under **Law 3917/2011**. The data can be provided only to the competent authorities in accordance with the procedure, the terms and the conditions of access set forth in Law 2225/1994 (Article 4). Thus the retained data **cannot be used for protecting intellectual property**. The Greek legislator has opted for the maintainance of data for a period of one year (Article 6).
Nevertheless, according to Article 5.5 of the Law 3471/2006 (as modified by the Law 4070/2012) *"the provider of publicly available electronic communications service must … enable the use and payment of these services anonymously or under a pseudonym"*.
The period of one year is also applied in French law, by Articles R. 10-13 and L. 34-1-III of the Code of Post and Electonic Communications (*Code des postes et des communications électroniques*, CPCE). This provision was entered into force before the enactment of the EU directive (by the Decree (*décret*) 2006-358 of 24.03.2006), so the French legislator had not to take additional measures to ensure compliance with the provisions of the Directive. According to this Article, technical data should be

retained *"for the purposes of finding, detecting and prosecuting criminal offenses, or breach of obligations, defined in **Article L. 336-3** of the Code of Intellectual Property, and in the sole purpose of making them available, as appropriate, to the judicial or executive authority (HADOPI) referred to in Article L. 331-12 of the Code of Intellectual Property"* (trans.). Article L. 336-3 provides for the subscriber's obligation to take safety measures in order to protect the use of its access service. Thus, in the French legal system, the retained data **can be used for intellectual property protection**.

The service provider should retain, in compliance with the above provisions, *"the name and **address of the subscriber or registered user to whom an Internet Protocol (IP) address**, user ID or telephone number was allocated at the time of the communication"* (Directive 2006/24/EC Article 5.2.iii). Furthermore, it should be underlined that under no condition the provider can retain the content of communication; an obligation to retain traffic or location data can only be imposed to him (see Directive 2002/58/EC Article 2 (b) and (c) for definitions of such data).

It is worth, however, referring to the reactions of the German Constitutional Court to the German law, providing similar measures, in order to put emphasis on the predominant role of the judicial intervention, in case of serious offences of privacy.

Regarding the duty of the providers of publicly accessible telecommunications services to keep subscribers' personal data, the German Constitutional Court on an interim judgement of 11 March 2008 found that **the use of data can only be made in judicial proceedings in progress**, for a particular serious violation (Press release no. 37/2008 of 19 March 2008, Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 256/08) [Press release no. 37/2008; Moritz, 2008]. In its judgement of 2 March 2010, the court confirmed that the use of personal data be allowed **only for safety reasons**. The court found the provision unconstitutional, by stating that *"**a duty of storage to the extent provided is not automatically unconstitutional at the outset**. However, it is not structured in a manner adapted to the principle of proportionality. The challenged provisions guarantee neither adequate data security nor an adequate restriction of the purposes of use of the data. Nor do they in every respect satisfy the constitutional requirements of transparency and legal protection"* (Press release no. 11/2010 of 2 March 2010, Bundesverfassungsgericht, 27.02.2008, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Data retention unconstitutional in its present form) [Press release no. 11/2010; Mareau, 2010]

It should be clarified that the legal obligation imposed upon providers to maintain personal data is not, however, applicable to search engines. The search engines are recommanded to maintain users' data for the shortest time possible, i.e. six months. This is thought to minimize risks of possible combination of the data being construed. Indeed, this was exactly the retention period proposed by Article 29 Data Protection Party in the **Opinion 1/2008** on data protection issues related to search engines [Article 29 Data Protection Party, 2008]. However, it should be noted that prior to this proposal, some search engines were retaining users' personal data for a period of 18-24 months [Waters, 2009; Sullivan, 2007].

2. Article 6-II and 6-III of the French Law 2004-575 : data retention for identification reasons

Article 6-II of the French Law 2004-575 imposes on service providers the obligation to **maintain data of users who contribute in creating content published on a**

website. The providers may have to communicate such data to a judicial authority. Article 6-III of that law, explicitly gives a list of data information which persons with a professional activity as a content editor should make available to the public. By contrast, individuals may retain anonymity; their data may not be published on a website; it suffices to provide this information to the provider. Therefore, hosting providers, such as "Dailymotion", "youtube.com", "eBay", should maintain the data of these users. Service providers are subject to professional confidentiality regarding any information leading to identifying the persons concerned; however, this privilege cannot be invoked before a judicial authority [Derieux, 2008]. Therefore, in a case whereby the content published on a website infringes intellectual property rights, the identification of the editor could be possible due to the data retention obligation imposed upon the provider, pursuant to Article 6-II [Szukin / Guillenshmidt, 2008].

Another issue raised was concerned with **which personal data** the providers had to demand from users and maintain. More analytically, if it was sufficient to maintain the **user's IP address**, based on the assumption that the user of the online service is the subscriber to the internet access service. The court held that it suffices to maintain only the e-mail address and IP address of the content editor, in the absence of the provided decree (*décret*) regarding the data to be maintained by a hosting service provider (TGI Paris, 07.01.2009, Jean-Yves Lafesse a.o / YouTube) [TGI Paris, 2009]. By contrast, as *Criqui* observes, the providers should maintain complete identity data (such as name, address, etc.) of the content editors, as required by Law 2004-575. The verifiability of this data has no effect on the editors' obligation to provide valid identification data, when acting in good faith [Criqui, 2009].

Further to the above, until recently, there was no legislative provision on whether a hosting **provider should confirm data provided by a user**. According to case-law, if the data declared by a user is obviously false, the provider should ask for evidence (i.e. Tribunal d'instance de Vienne, 12.11.2010, Vincent M. v eBay International AG) [Tribunal d'instance de Vienne, 2010]; CA Paris, 07.06.2006, Tiscali Média v Dargaud Lombard, Lucky Comics [CA Paris, 2006]). However, the Supreme Court refused to impose upon providers an additional obligation, given that the law does not require the verification of the identification data (Cass. civ., 14.01.2010) [Cass., 2010]. Other judgements of the courts of first instance have confirmed the provider's obligation to retain data, but **not to verify them** (TGI Grenoble, 01.02.2007, Jean-Pierre Contoz c/Sté eBay international) [TGI Grenoble, 2007; E-commerce et escroquerie : irresponsabilité d'eBay, 2007]. Furthermore, a judgement concluded the presence of providers' negligent conduct resulting in depriving the victims of suing against infringers; thus, a tort under Article 1383 of *Code Civil* was established (TGI Paris, 16.02.2005, Sté Dargaud a.o. v Sté Tiscali Media) [TGI Paris, 2005].

In any case, the **Decree 2011-219 of 25 February 2011**, issued seven years after the publication of the law providing for its issuance, **listed personal data to be maintained** [Castets-Renard, 2011]. It includes the bank reference of the payment as well as the payment amount regarding a paid e-service. However, data processing aiming at identifying the users hardly justifies maintaining all this information [Chafiol-Chaumont, 2011]. Moreover, it is not justified to maintain the password for access to electronic services [Grégoire, 2011]. These passwords are normally encrypted, so they remain unknown to the provider. An additional risk is also the standard use of the same password to several different online services. Therefore, the invasion of a users' privacy can take a heavy toll in the case of theft of these codes [Chafiol-Chaumont, 2011].

The data retention period provided by the decree is one year (Article 3). That is exactly the same period as foreseen in Articles L. 34-1 and L. 34-1-III CPCE. There is also a provision to cover the excessive cost of providers due to this requirement. It is worth referring to the **Decision of the *Conseil Constitionnel*** 2000-441 (28.12.2000) stating that *"in compliance with the constitutionally guaranteed freedoms, requiring operators of telecommunications networks to establish and operate the technical devices that permit interceptions justified by the needs of public safety, and to contribute in safeguarding the public order, in the general interest of the population, is outside the scope of the operation of telecommunications networks; therefore, the operators **should not cover directly the above resulting costs**, given the nature of these actions"* (trans.). In addition, the competitive disadvantage to small providers, who will possibly have to pay a disproportionate amount in relation to their infrastructure, in order to maintain all this data, should not be ignored.

3. LOPPSI 2 : data retention for strengthening national security

The recent French **Law 2011-267** of 14 March 2011 on guidance and planning for the strengthening of national security (*loi d'orientation et de programmation pour la perfomance de la sécutité intérieure*, LOPPSI 2) enables **remote access to a user's computer** for detection of certain crimes, if allowed by a judge, for a maximum period of four months (Article 36). In no case is it allowed that this law be applied to intellectual property infingements.
By contrast, the German Constitutional Court, in its judgement of 27 February 2008, refused to allow the remote access to a user's computer and established the principle of guaranteeing the confidentiality and the integrity of information systems. The court found that there is a breach of the principle of proportionality of the measures available to authorities, to gain access to information, when their obligations are not clearly specified (Press release no. 22/2008 of 27 February 2008, Bundesverfassungsgericht, 1 BvR 370/07 1 and BvR 595/07) [Press release no. 22/2008; Guerrier, 2011].

We conclude, that, while, in principle, the retention and the **subsequent processing of personal data was the exception**, following the adoption of Directive 2006/24/EC, of the Greek Law 3917/2011, of the French Decree 2006-358, of the French law 2011-267, it **has become the rule**. Before the adoption of the Directive, the **EDPS** had not been convinced **of the necessity** to impose an obligation upon the service providers to retain personal data. The EDPS also proposed that the duration of data retention should be limited to 6-12 months instead of the initially proposed period of two years [EDPS Press Release, 2005]. However, by invoking the need to combat criminal activity, especially after the terrorist attacks in New York, Madrid and London, the European legislator overcame the reactions expressed regarding the restriction of privacy.
Moreover, as *Lorrain/Mathias* observe, *"The severity of the law imposes on the economy a significant risk of offshoring activities of providers outside the borders of the European Union"* (trans.) [Lorrain / Mathias, 2007].

Concluding remarks

The protection of intellectual property (Article 17 of the Greek Constitution, Article 2 and 17 of the French Declaration of the Rights of Man and of the Citizen) is **in conflict** with the protection of **privacy** (Article 9 of the Constitution, Articles 2 and 4 of the Declaration, Article 8 ECHR, Article 7 of the Charter of Fundamental Rights of the European Union), the protection of **personal data** (Article 9A of the Constitution, Articles 2 and 4 of the Declaration, Article 8 ECHR, Article 8 of the Charter of Fundamental Rights of the European Union), the **freedom of expression** (Article 14 of the Constitution, Article 11 of the Declaration) and the **communication confidentiality** (Article 19 of the Constitution, Articles 2 and 4 of the Declaration). The result of the conflict is left to national regulators, since the Court of Justice of the European Union declined to resolve the issue at European level. The national regulators should take into account the general principles of proportionality and of necessity.

Under *Greek* law, **the waiving of confidentiality for *intellectual property infringements* is not allowed**; thus disclosure of the users' data is not allowed under any circumstances in order to investigate such offenses.
Under *French* law, the courts and the collecting societies can **process data** regarding offences, in respect to other laws, namely the **Law HADOPI**. Thus the HADOPI authority may process users' data in order to send letters to subscribers informing them of intellectual property infringements committed by them. Therefore, the rightholders have no access to users' data without judicial intervention and users' privacy is adequately protected.

As indicated above, the main debatable issue, as was addressed in this paper, is the existing conflict between intellectual property and personal data protection. A further issue that the paper addresses is the area whereby conflict does not exist (second area). There is also a third area, where intellectual property and personal data are in a degree of conflict but can neverthless be reconciled.
The second area concerns the works available with **licenses Creative Commons** (CC) as well as the open source software. The CC licenses contain various terms of the licensed use, i.e. providing attribution to the original creator and licensor (BY), prohibiting the commercial use of the work (NonCommercial, NC), permitting reuse provided the work is not modified (NoDerivatives, ND), allowing modifications and, requiring modified works to be released under the same license (ShareAlike, SA) [About the licenses, 2012; Frequently asked question, 2012]. As for the **open source software**, the licensed use varies depending on the granted license, i.e. the GNU GPL license (General Public Licence of Free Software Foundation) allows modifying the software, requiring the licensee to disclose the source code in case of further redistribution [Cool / Laurent, 2005]. Therefore, in these cases, there is no intellectual property infringement since the use of works is in accordance with the conditions laid down therein. The Greek as well as the French "creativecommons" website (but no the "www.creativecommons.org") clearly state that **licensed CC works can be exchanged via file-sharing networks**. To be more analytical, the Greek website states that *"All Creative Commons licenses explicitly provide for an exception for file sharing. The licenses provide that exchanging works via the internet (online) is not a commercial use, if it is not taking place for an economic advantage"* (trans.) [Application of Creative Commons, 2012]. On the French website, it is mentionned

that *"The aim is to encourage a simple and lawful circulation of works, the exchange and the creativity; thus, the sharing of works, on P2P networks (peer-to-peer) or otherwise, is permitted"* (trans.) [FAQ, 2012]. Therefore, there is no need to disclose users' personal data in case of exchanging works bearing such licenses.
In the second case, the rightholders of these works have, in principle, exclusive rights. It is, however, possible to sign **agreements with platforms** on which their works are available **in exchange for a fee**. Such an agreement also takes into account the interests of all parties. The interests of rightholders are taken into account: they receive remuneration for making available their works on the platforms and benefit from greater visibility of their works. We could just think that there are artists, who allow access to their works, even for free, in order to become quickly known by a wider audience. Others favour the free movement of ideas and creations, sharing them with all the online community, inspired by Open Source Initiative [The Open Source Definition, 2007]. It should be clarified that Open Source Initiative differs from Free Software Foundation. The first one supports the idea that a work belongs to the community. Therefore, no royalty or other fee should be required. The second one argues that using the word "free" does not mean offering without charge, but offering a work with the source code [Renard, 2000; Roquefeuil, 2007; Avgerinos/Tsavos, 2006]. On the other hand, the interests of the platforms are also taken into account: they provide richer content to the public. Thus, a large audience wishing to have access to these platforms results in increased revenue from advertising. For instance, the platform Dailymotion has already concluded agreements, from 18 October 2007, with collecting societies, to make available works of creators managed by these societies on the internet, by paying a determined fee [de Martino, 2008]. However, *Sirinelli* was not convinced of the efficacy of this agreement and has pointed out that signing an agreement between platforms and collecting companies managing intellectual property in animation is inadequate, since an agreement of related rights holders (singers, musicians, actors, etc.) is also required. Otherwise, the rights of the latter would be infringed [Sirinelli, 2009].

These agreements offer one more benefit to the platforms. They help platforms to be exempted from any liability for intellectual property infringement and from any obligation to take filtering action. In principle, the platforms as hosting service providers, are not liable for the contents published on the platform if they are unaware of it (i.e. if they have not received notification for illegal content). In addition, despite decisions by national courts imposing a filtering obligation on platforms or the obligation to take safety measures, in order to prevent intellectual property infringements (CA Paris, 09.11.2007, eBay v/ DWC [Saint-Martin, 2007]; TGI Troyes, 04.06.2008 [Saint-Martin, 2008]; TGI Paris, 13.07.2007, Nord Ouest Production v/ SA Dailymotion [Tabaka, 2007]), the Court of Justice of the European Union ruled, in case *Scarlet Extended SA v SABAM a.o.* (Judgement of 24 November 2011, C-70/10), that **a general filtering obligation cannot be imposed on service providers** [Troianiello, 2012]. According to the Court, it cannot be required from the provider *"to install a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software"*. Furthermore, the Court has stated, in case *L'Oréal SA a.o. v eBay International AG a.o.* (Judgement of 12.07.2011, C-324/09), that *"the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website. Furthermore, a general monitoring*

obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly". The possible imposition of a filtering obligation provided in the draft law HADOPI 1 had been eventually removed as it was not possible to determine clearly the filtering measures nor to estimate the cost of implementing these measures [M. Colaud, 2009]. This paper has also referred to the first judgement of a Greek court ordering the provider to take **technological measures** regarding specific webpages (see above p. 8 last paragraph) [Court of First Instance of Athens, 2012].

In addition, **filtering content** on a website by using methods as digital watermarking, audio or image fingerprints is a wide spreading technique available for the protection of intellectual property, i.e. technology "Audible Magic" used by MySpace and Facebook, "Signature" technology used by Dailymotion, "content ID" used by YouTube. **Education of users** so as to respect others' rights, i.e. the letters sent by the HADOPI authority or educational messages on websites, is also of essential importance in order to protect intellectual property [Audible Magic, 2011; Dailymotion, 2008].

Moreover, in French legal system, a discussion for a system of "**global license**" (*licence globale*) was launched, during the drafting of the Law DADVSI (see above p. 12 first paragraph), that makes it possible for users to pay providers a fee, redistributed to rightholders, depending on the volume of downloaded works [Thoumyre, 2006]. Finally, the proposal was rejected due to the reactions to it. A similar discussion was open in Belgium [Lalieux, 2010].
However, there is no intellectual property infringement, if we accept for downloads the **exemption for private use** (i.e.TGI Paris, 08.12.2005, the court held that the accused had no information as to whether the works are protected by intellectual property) [Thoumyre, 2006]. This exemption is not accepted by the case-law in the most cases. It seems that the exemption of private copying cannot result in making legal the reproduction of an illegally acquired work (i.e. Tribunal de Grande Instance de Rennes, 30.11.2006) [TGI Rennes, 30.11.2006; Thoumyre, 2007]. However, it has been argued that making lawfully a copy for private use does not require the possession of the original work or of an authorized copy [Macrez, 2005]. In addition, downloading via file sharing networks does not meet the requirements of the three step test (Berne Convention for the Protection of Literary and Artistic Works Article 9.2, Directive 2001/29/EC Article 5.5, Law 2121/1993 Article 28.C, Articles 122-5 and 211-3 CPI), since such reproduction conflicts with a normal exploitation of the work and unreasonably prejudices the legitimate interests of the creator.
Furthermore, rightholders can use technological measures designed to prevent or restrict acts not authorized by them (see Paragraph 47, Preamble to the Directive 2002/29/EC). However, *"any such rights-management information systems … may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour"* in compliance with Directive 95/46/EC (Paragraph 57, Preamble to the Directive 2002/29/EC).

Of particular interest is the **ACTA** (Anti-Counterfeiting Trade Agreement), already signed (but not ratified) by Australia, Canada, Japan, South Korea, Morocco, New Zealand, Singapore and the United States. The European Commission and its Member States (22 of them) signed this Agreement on 26.01.2012 [Contrefaçon : l'Union

Européenne signe le Traité ACTA, 2012; Signing Ceremony for the Anti-Counterfeiting Trade Agreement (ACTA), 2012]. However, it should also be approved by the European Parliament in order to become a committed text for the European Union. The European Commission had proceeded with negotiations with other parties, without having informed the European Parliament. Apart from the secrecy of the negotiations, reactions were also caused because the text under negociation came to public attention only during the final stage of negociations, whereas Article 207.3 of TFEU provides that *"The Commission shall report regularly to the special committee and to the European Parliament on the progress of negotiations"* [ACTA: appel du Parlement européen à la transparence, 2010]. It should be noted, however, that the most of the provisions which caused reaction were deleted in order to reach agreement. Thus, the gradual process of notification (the "three strikes" system) in order to impose the interruption of internet access service was not adopted. As for the subscribers' identification, **states may require providers to disclose the personal data** of copyright or related rights infringers (Article 27.4). Furthermore, Article 23.1 refers to copyright and related rights piracy on a commercial scale, without providing explicitly for exceptions that should be considered as fair use (i.e. private copying, use for criticism or teaching).
All this discussion for ACTA takes place at a time when U.S. Congress seems to abandon **SOPA** (Stop Online Piracy Act) and **PIPA** (Protect Intellectual Property Act) because of the reactions that the restrictions imposed on free use of the internet have caused at the other side of the Atlantic Ocean. The two acts have allowed in their proposals that the Ministry of Justice could publish lists of problematic websites (black lists) and could command internet service providers to block access to these sites. Furthermore, rightholders could demand that the providers take preventive measures upon a simple notification, while the latter could be relieved of their liability of blocking innocent sites [Les geeks font plier le Congrès, 2012].

Finally, it is possible that the European Parliament will not approve ACTA. The digital agenda commissioner Neelie Kroes admitted *"We are now likely to be in a world without [the stalled US act] SOPA and without ACTA. Now we need to find solutions to make the internet a place of freedom, openness, and innovation fit for all citizens, not just for the techno avant-garde"* [David Meyer, 2012]. A condition of freedom, openess and innovation is the protection of users' privacy.

References

Avgerinos G. / Tsiavos Pr. (2006), The Open Source Licenses (free / open source licences) as a conventional form of organizing productive activity (Greek), Media and Communications Law "ΔιΜΕΕ", 169-180.

Benabou V.-L. (2009), Close de la loi HADOPI ou opération nécessaire de débrouissaillage (après la censure du Conseil constitutionnel du 10 juin 2009, Revue Lamy Droit de l'Immatériel "RLDI", 52, 63-73.

Bensoussan A. (2007), La CNIL désavouée sur la question du peer to peer, Informatique, 22.06.2007, 54, online at www.alain-bensoussan.com/accessed 27.05.2012.

Bitan H. (2009), Réflexions sur la loi « Création et Internet » et sur le projet de loi « HADOPI 2 », RLDI, 51, 121-126.

Boubekeur I. (2009), De la « loi HADOPI » à la « loi HADOPI 2 », RLDI, 51, 107-128.

Caron Ch. (2007), Qualification de l'adresse IP : état de lieux jurisprudentiel, Communication -Commerce Electronique, 12, comm. 144, 32-35.

Caron Ch. (2009), Validité des constats effectués par des agents assermentés, Communication-Commerce Electronique, 4, comm. 31, 25-26.

Castets-Renard C. (2011), Publication du décret d'application relatif à la conservation et à la communication des données d'identification à la charge des prestataires techniques : enfin, RLDI, 70, 81-85.

Chafiol-Chaumont Fl. (2011), Retour sur l'obligation de conservation des données d'identification après la parution du décret du 25 février 2011, RLDI, 71, 57-60.

Chafiol-Chaumont Fl. / Bonnier A. (2009), L'identification des « pirates du web" à partir de leur adresses IP, RLDI, 49, 84-89.

Chavent-Leclère A.-S. (2011), La responsabilité pénale à la lumière des lois « Hadopi », RLDI, 67, 79-80.

Colaud M. (2009), L'adoption au Sénat du projet de loi « Création et internet » : la confirmation d'une méthode de régulation consensuelle en propriété littéraire et artistique, RLDI, 46, 85-93.

Couland M. / Mariez J.-S. (2008), L'évolution de la protection des oeuvres sur les réseaux numériques ou le choix du mode contractuel, RLDI, 34, 53-65.

Cool Y. / Laurent Ph. (2005), Introduction générale : repères pour comprendre le mouvement du logiciel libre, in Les logiciels libres face au droit, Cahiers du Centre de Recherches Informatique et Droit, 1-22.

Criqui G. (2009), La fourniture d'une simple adresse IP est-elle suffisante ? Ou quand l'obligation d'identification à la charge de l'hébergeur doit être précisée, RLDI, 49, 74-77.

Derieux E. (2008), Internet et protection des données personnelles, RLDI, 38, 75-85.

Drouard E. (2007), Peer-to-peer, sociétés d'auteurs et CNIL, RLDI, 29, 59-61.

Dupuis M. (2001), La vie privée à l'épreuve de l'Internet : quelques aspects nouveaux, RLDI, 12.

Forest D. (2011), Droit d'auteur et données personnelles Un marriage morganomique ?, RLDI, 69, 80-89.

Frescaline A. (2012), Ce que les candidats pensent d'Hadopi, online at lci.tf1.fr/ accessed at 27.05.2012.

Gautron A. (2009), La réponse graduée (à nouveau) épinglée par le Conseil costitutionnel, RLDI, 51, 63-73.

Gitton A. (2008), HADOPI – DADVSI II – Riposte graduée, RLDI, 41, 63-73.

Grégoire St.(2011), Le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne Premières lectures d'un décret attendu six ans …, RLDI, 70, 86-91.

Guerrier Cl. (2010), "Loppsi 2" et l'utilisation des nouvelles technologies, RLDI, 64, 70-82.

Guerrier Cl. (2011), La "Loppsi 2" en 2011, RLDI, 70, 92-101.

Guerrier Cl. (2011), Captation de données et vie privée en 2011, online at http://www.juriscom.net/accessed 27.05.2012.

Heinich J. (2011), La nouvelle obligation de surveillance de sa ligne : nouvelle responsabilité civile?, RLDI, 67, 75-78.

Hollande Fr. (2012), La loi Hadopi doit être repensée, online at www.lemonde.fr/accessed at 27.05.2012.

Kallinikou D. (2010), Intellectual Property, Privacy and Personal Data (Greek), 27.11.2010, online at www.icsd.aegean.gr/accessed 27.05.2012.

Lalieux K. (2010), Téléchargement illegal : Faut-il légiférer, 25.01.2010, online at http://www.karinelalieux.be/accessed 27.05.2012.

Lorrain A.-C. / Mathias G. (2007), Conservation des données de connexion : un projet de décret reserre la toile … ou comment l'ombre de « Big Brother » menace la « confiance dans l'économie numérique », RLDI, 28, 39-45.

Macrez Fr. (2005), A l'abordage des pirates. A propos du jugement du Tribunal de grande instance de Pointoise du 2 février 2005, RLDI, 3, 14-17.

Macrez Fr. / Gossa J. (2009), Surveillance et sécurisation : ce qui l'Hadopi rate, RLDI, 50, 79-91.

Mareau E. (2010), Liberté ou sécirité ? Karlruhe tranche, online at www.lagazettedeberlin.de/accessed 27.05.2012.

Martino (de) G. (2008), Table ronde II – La coopération, une nécessité pour réguler internet. La nouvelle attribution des rôles doit-elle conduire a la révision de la directive e-commerce ?, RLDI, 43, 88-90.

Mélin M. / Melison D. (2007), Salarié, employeur et données informatiques : brefs regards croisés sur une pièce à succès, 2007/01/01, 23, 69-75.

Meyer D. (2012), ACTA likely to fail, European Commission admits, 04.05.2012, online at www.zdnet.co.uk/blogs/2012/accessed 27.05.2012.

Moritz L. (2008), Les perquisitions en ligne et la surveillance d'internet, RLDI, 41, 53-62.

Papadopoulos M. (2007), Legal Problems in Waiving of Privacy protection and secrecy of Communications as foresees by the Law in Greece, online at www.marinos.com.gr/accessed 27.05.2012.

Pignatari O. (2010), Téléchargement illicite d'oeuvres musicales : l'articulation toujours délicate avec les données et le rejet persistant de la copie privée, no 60, 14-18.

Putman E. (2011), La "preuve par l'adresse IP" : une vraie question … déjà dépassé?, RLDI, 2011, 67, 84-86.

Renard I. (2000), Licences « open source » : la fin des redevances ?, PA, 205, 13 oct., 17.

Roquefeuil B. (2007), Le statut juridique des logiciels libres : un régime juridique qui n'est pas unifié, GP, 18, 18 janv., 10.

Saint-Martin A. (2008), eBay responsable de son site… Première application d'une responsabilité raisonnable pour le web 2.0 ?, RLDI, 39, 44-50.

Saint-Martin A. (2007), Une obligation de surveillance limitée pour les gestionnaires de plates-formes Web 2.0, RLDI, 33, 46-47.

Simon Ch. (2009), Les adresses IP sont des données personnelles selon le Conseil constitutionnel, RLDI, 51, 114-115.

Sirinelli P. (2009), La responsabilité des prestataires de l'internet : l'exemple des sites contributifs, RLDI, 49, 78-83.

Sotiropoulos V. (2012), An analysis of ACTA (Greek), 21.02.2012, online at www.elawyer.blogspot.com /accessed 27.05.2012.

Sotiropoulos V. (2009), The Opinion of Sanida under the microscope (Greek), 30.06.2009, online at www.elawyer.blogspot.com/accessed 27.05.2012.

Strugala Cl., La protection de la personnalité à l'épreuve du numérique, RLDI, 66, 49-56.

Sullivan D. (2007), Google Anomymizing Search Records to Protect Privacy, online at searchengineland.com/accessed 27.05.2012

Synodinou T.-E. (2010), Intellectual Property Law and Data Protection, in Protecting Privacy & Information and Communications Technologies (Greek), 603-628.

Synodinou T.-E. (2008), Intellectual Property and New Technologies (Greek).

Szuskin L. (2007), Les titulaires de droit d'auteur, laissés pour compte de la lutte contre la piraterie sur internet?, RLDI, 29, 61-63.

Szuskin L. (2009), « Sans contrefaçon » ? Une étude comparée de la lutte contre le piratage en ligne des droits d'auteur et voisins, RLDI, 50, 70-78.

Szukin L. / Guillenshmidt (de) M. (2008), L'arrêt « Promusicae » : beaucoup de bruit pour rien ?, RLDI, 37, 6-8.

Tabaka B. (2007), Commerce électronique : les plates-formes sont-elles hébergeurs?, RDLI, 33, 10-15.

Tafforeau P. (2011), Les lois « Hadopi » et la protection des droits d'auteur et droits voisins sur internet, RLDI, 74, 112-116.

Taylor R. (2010), The Digital Economy Act 2010 and online copyright infringement, 09.09.2010 online at http://www.lawgazette.co.uk/accessed 27.05.2012.

Thoumyre L. (2006), Les faces cachées de la décision du Conseil constitutionnel sur la loi « DADVSI », RLDI, 20, 6-17.

Thoumyre L. (2006), Peer-to-peer : un « audiopathe » partageur relaxé pour bonne foi, RLDI, 16, 23-26.

Thoumyre L. (2007), Arrêt d'Aix-en-Provence du 5 septembre 2007 : de la copie privée à la privation de copie ?, RLDI, 31, 10-14.

Thoumyre L. (2006), La licence globale optionnelle : un pare-feu contre les bugs de la répression, 15, 80-84.

Troianiello A. (2012), La CJCE s'oppose au filtrage généralisé de l'Internet, RLDI, 78, 71-75.

Tsolias Gr. (2004), The telecommunication data in light of confidentiality: concerns in view of the incorporation of the Directive 2002/58/EC (Greek), ΔιΜΕΕ 2004, 357-370.

Waters D. (2009), Wiping data 'hits flu prediction', 19.05.2009, online at http://news.bbc.co.uk/accessed 27.05.2012.

Identification des utilisateurs de logiciels d'échanges pair à pair par leurs adresses IP, (2008), J.-B.A., RLDI, 35.

E-commerce et escroquerie : irresponsabilité d'eBay (2007), RLDI, 29, 56.

ACTA: appel du Parlement européen à la transparence (2010), RLDI, 59, 22-23.

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN, WP 136, http://ec.europa.eu/justice/policies/privacy/accessed at 27.05.2012.

Article 29 Data Protection Working Party, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, adopted on 30 May 2002, 10750/02/EN/Final, WP 58, online at http://www.eu.ipv6tf.org/PublicDocuments/accessed at 27.05.2012

Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, 04.04.2008, 00737/EN, WP 148, p. 19, online at http://ec.europa.eu/justice/policies/privacy/docs/accessed at 27.05.2012.

Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010/C 147/01) [online at http://www.edps.europa.eu/accessed 27.05/2012

Greek Prosecutor's Opinion 9/2009, online at dsanet.gr/accessed 27.05.2012.

Press release no. 22/2008 of 27 February 2008, Bundesverfassungsgericht, 1 BvR 370/07 1 and BvR 595/07, Provisions in the North-Rhine Westphalia Constitution Protection Act (*Verfassungsschutzgesetz Nordrhein-Westfalen*) on online searches and on the reconnaissance of the Internet null and void, online at www.bundesverfassungsgericht.de/accessed 27.05.2012.

Press release no. 37/2008 of 19 March 2008, Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 256/08, Application for a temporary injunction in the matter of "data retention" succeeds in part, online at www.bundesverfassungsgericht.de/accessed 27.05.2012, online at www.lagazettedeberlin.de/accessed 27.05.2012.

Press release no. 11/2010 of 2 March 2010, Bundesverfassungsgericht, 27.02.2008, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Data retention unconstitutional in its present form, online at www.bundesverfassungsgericht.de/accessed 27.05.2012.

EDPS Press Release, Data retention: EDPS presents his Opinion on the Commission proposal for a Directive 2005, EDPS/05/5, 26.09.2005, online at www.edps.europa.eu/accessed 27.05.2012.

Contrefaçon : l'Union Européenne signe le Traité ACTA, 26.01.2012, online at www.lemonde.fr/accessed 27.05.2012.

Signing Ceremony for the Anti-Counterfeiting Trade Agreement (ACTA), 26.01.2012, Ministry of Foreign Affairs of Japan, online at www.mofa.go.jp/accessed 27.05.2012.

European Digital Rights, ACTA and its impact on fundamental rights, 02.02.2012, online at www.edri.org/accessed 27.05.2012.

Les geeks font plier le Congrès, 2012, 25.01.2012, online at www.lemonde.fr/accessed 27.02.2012.

About the licenses, online at http://creativecommons.org/licenses/accessed 27.05.2012.

Frequently asked question, online at http://creativecommons.org/licenses/accessed at 27.05.2012.

Application of Creative Commons, question "May I obtain a pecuniary advantagefrom a work that becomes accessible to the public under license Creative Commons?" (trans.), online at ww.creativecommons.gr/accessed 17.05.2012.

FAQ, 1/ Pourquoi utiliser une licence Creative Commons ? online at http://creativecommons.fr/accessed 27.05.2012.

The Open Source Definition, online at http://www.opensource.org/accessed 27.05.2007.

Digital Economy Act 2010, online at http://www.legislation.gov.uk/accessed 27.05.2012.

Audible Magic Awarded Patent for Technology That Identifies Content Played on Smart Phones, Smart TVs, and other Media Devices, 20.07.2011, online at http://audiblemagic.com/accessed 27.05.2007.

Dailymotion Announces Full Implementation of INA Technology for Detection of Copyrighted Video, 25.02.2008, online at http://press.dailymotion.com/fr/accessed 27.05.2007.

Court of First Instance of Athens, no 4658/2012, 16.05.2012, online at www.nb.org/blog/wp-content/accessed 27.05.2012.

Tribunal de Grande Instance de Rennes, 30.11.2006, online at www.legalis.net/accessed 27.05.2012.

CA Douai, 26.11.2004, online at www.foruminternet.org/specialistes/veille-juridique/jurisprudence/accessed 27.05.2012.

TGI Paris, 07.01.2009, Jean-Yves Lafesse a.o / YouTube, online at www.legalis.net/accessed 27.05.2012.

Tribunal d'instance de Vienne, 12.11.2010, Vincent M. v eBay International AG, online at www.legalis.net/accessed 27.05.2012.

CA Paris, 07.06.2006, Tiscali Média v Dargaud Lombard, Lucky Comics, online at www.legalis.net/accessed 27.05.2012.

Cass. civ., 14.01.2010, online at www.legalis.net/accessed 27.05.2012.

TGI Grenoble, 01.02.2007, Jean-Pierre Contoz c/Sté eBay international,n online at www.droit-technologie.org.

TGI Paris, 16.02.2005, Sté Dargaud a.o. v Sté Tiscali Media, online at www.legalis.net/accessed 27.05.2012.

TGI Paris, 24.06.2009, Jean-Yves Lafesse a.o. v Google, online at www.legalis.net/accessed 27.05.2012.

Cass. crim., 13.01.2009, no 08-84088, onlime at www.legifrancefr/

Decisions of the *Conseil Constitutionnel* onlime at www.conseil-constitutionnel.fr/