INTERNATIONAL HELLENIC UNIVERSITY

Reconciling the rising tensions between Data Protection and Intellectual Property in the digital age - a European Law approach

Aikaterini Tsintza

Supervisor: Dr. Panagiotis Kitsos

Dissertation submitted in fulfillment of the requirements of the degree of

Master of Laws (LLM)

in Transnational and European Commercial Law and Alternative Dispute Resolution

School of Economics & Business Administration

International Hellenic University

21 December 2013

To my family

ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to my supervisor, Dr. Panagiotis Kitsos, whose expertise, understanding and patience added considerably to my postgraduate experience and his continuous support, his invaluable suggestions and guidance helped me in all stages of the research and writing of this LLM study.

Besides my supervisor, I would like to thank Professor Dr. Athanasios Kaissis for his motivation, enthusiasm, genuine caring and immense knowledge and especially for offering us a chance to get acquainted with contemporary and emerging legal procedures by experts from all over the world.

A very special thanks goes to the academic assistants, Stavroula Angoura and Dr. iur. Komninos Komnios, for their patience, understanding and support and for always being there for us, as well to as all the academic and administrative staff and the librarians of the International Hellenic University for making this journey possible.

Besides, I would like to acknowledge the International Hellenic University - School of Economics and Business Administration. My postgraduate experience benefitted greatly from the courses I took, the opportunities I had and the high-quality lectures that the department organized.

I am, also, deeply indebted to my family and friends, without the love, the support, the patience, the understanding and the encouragement of whom, I would not have been able to complete my post-graduate studies nor this dissertation.

ABSTRACT

This study regards a brief overview of the legal situation regarding the interaction between personal data protection and intellectual property at the European Union level.

The first section addresses the issue of the concept of personal data protection. In particular, it analyzes the naissance and evolvement of the rights of privacy and personal data protection, the European legal framework, the influence of the digital age over them, as well as the issue of the IP addresses which may be considered or not as personal data.

The second section analyzes issues regarding the intellectual property rights. More precisely, it analyses the definition and evolution of intellectual property rights, the European regulatory framework of copyright protection and it presents the implications of technology in the intellectual property rights, through the emergence of the internet, digital piracy, peer-to-peer file-sharing. Lastly, it deals with the issues of the ISPs' liability and the DRM as a means to protect copyright.

The third section addresses the issue of the interaction of data protection and online copyright enforcement and of whether the European legal framework for data protection presents a barrier to the fight against online copyright infringement, on the basis of the pertinent case-law and more precisely the Peppermint and Promusicae cases.

The methodology of preparing this study is based on a pertinent EU law (primary and secondary) analysis of personal data protection and intellectual property rights protection, on the case law concerning the collision of these two fundamental rights, opinions of national data protection authorities, as well as the relevant literature (books and articles).

TABLE OF CONTENTS

1.- INTRODUCTION

The digital era we live in has created a new perspective regarding the protection of fundamental rights, due to the new technology and especially the recently invented internet and the massive access of population to the worldwide system of communications, which have managed to affect and dominate every possible aspect of people's daily life in an unprecedented way.

New technology has created new behaviors; the distinction between private and public sphere has been muddled up; individuals reveal personal information online; they socialize online; they do business online; they accept location tracking; they become objects of profiling; information flows easily, instantly and often without authorization; activities that jeopardize fundamental rights, such as the right of privacy and data protection.

Furthermore, the aforementioned features, combined with the multi-purpose nature and the constantly evolving state of online services, have facilitated illegal activities to take place in an online environment.

Citizens acting regularly lawfully "commit massive infringements of copyright and related rights in the form of illegal up-loading and disseminating protected content"[1], when they act as internet users. It is characteristic that according to a report drafted by the International Federation of the Phonographic Industry (IFPI) nearly one in four active internet users in Europe visits unlicensed sites monthly[2]. The internet is full of illicit copies of copyright works, affecting negatively the creative industries and especially the music and film industries, causing them in particular a decrease of their sales and a loss of their revenue.

[1] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights, SEC(2010) 1589final, p. 5.

[2] IFPI Digital Music Report 2011 "Music at the touch of a button"', p. 14. Report available at the IFPI website: http://www.ifpi.org/content/library/DMR2011.pdf (accessed 15 February 2012).

In view of all these, copyright holders have tried to fight online piracy ineffectively, as proceeding to litigation against innumerable anonymous users proved costly, time-consuming and, in the end, futile.

In the meanwhile, new more effective ways of disseminating copyright material constantly emerge, forcing, thus, right holders to turn against intermediaries asking sometimes for damage restoration and others for the reveal of the identities of their subscribers acting illicitly, in order to be able to identify who the infringers are.

Intermediaries (Internet Service Providers), from their part, argue ferociously their liability for users' copyright infringements, on the grounds that it is not possible to monitor and filter their services; besides, they are reluctant to disclose personal data to the detriment of their customers, jeopardizing to lose their clientele and exposing to risk the individuals' right to privacy.

Community law and jurisprudence could not remain passive observers of the situation arising in the inner market in electronic communications sector, as two fundamental rights, not related much one another until now, the right to privacy or personal data and the right to intellectual property are especially involved.

2.- DATA PROTECTION IN THE DIGITAL AGE

2.1.-The naissance and evolution of the Right to Privacy

The origins of the right to privacy date back to ancient Athens, where privacy and property were interconnected and recognized as such, according to that period's law and writings[3].

Later on, the American lawyers Warren and Brandeis in an article published in 1890 in the Harvard Law Review pleaded for an independent right to privacy, as a right of individuals not to have personal information exposed to general public by instantaneous photographs, newspaper enterprise portrait circulation and gossip[4].

The official acknowledgment of the right to privacy came in 1939, as it was included into the American treatise, Restatement of the Law of Torts, which was recognized by almost all states of America, whereas Europe dealt for the first time with that right much later, in 1950, by including it into the European Convention on Human Rights (ECHR)[5].

Since then, many other international regulations have also recognized the right of privacy as well, such as in the case of Article 17 of the United Nations International Covenant on Civil and Political Rights, Article 12 of the Universal Declaration of Human Rights, Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[6], OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Directive 95/46/EC, Directive 2002/59/EC, etc[7].

Apart from its official acknowledgment, the content of the right to privacy or the right for every individual to experience a private life has evolved over time, from

[3] Moore, B., Jr. (1984). *Privacy: Studies in Social and Cultural History.* Armonk, N.Y.: M. E. Sharpe. pp. 82, 108 and 124.
[4] Warren & Brandeis. (1890). The right to privacy. *Harvard Law Review. Vol IV no 5*.
[5] European Convention of Human Rights and Fundamental Freedoms. 4 November 1950, 213 U.N.T.S.
[6] Council of Europe. 28 January 1981. European Treaty Series- No. 108.
[7] Yali, T. *Copyright and privacy: Their Interaction in the Context of Peer-to-peer Networks.* (Master thesis). Leiden University, Holland. pp. 23 and 24.

the right to be left alone[8], to the right to control information and to the right of development of the personality[9].

In Europe, there exists no established definition of "privacy", as it has multiple meanings depending on context and interpretation, ranging from bodily privacy (to protect the integrity of the physical person), territorial privacy (to protect personal space, objects and behavior), communications privacy (to protect against eavesdropping), location privacy (to protect against surveillance) and information privacy (to protect personal data)[10].

Up until the sixties, the private sphere was mainly concerned with the physical spaces in which an individual was able to retreat to from the world outside, such as the house and other private places[11]. But, due to technological developments on the registration of personal data in the sixties, the scope of the right to a private life has changed radically, introducing concepts such as the "informational privacy", referring to details about our lives that we would most often like to keep free from public view[12].

2.2.- Personal data: a European approach

The genesis of modern legislation concerning personal data in Europe and globally can be traced to the law enacted in the Land of Hesse in Germany in 1970, followed by the Swedish Data Act three years later, making Sweden the first country to adopt national legislation on the processing of data.

The enactment of these first generation norms was the evolution of two crucial international instruments: the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Organization for Economic Cooperation and Development's (OECD) 1980

[8] Warren & Brandeis, supranote 4.
[9] Wong, R. (2004). Privacy: charting its developments and prospects. *Human rights in the digital age. The Glasshouse Press (London)*. p. 148.
[10] Santucci, G. (2013). Privacy in the Digital Economy: Requiem or Renaissance? *The Privacy Surgeon*. Retrieved from http://www.privacysurgeon.org/blog/resources/gerald-santucci-paper/.
[11] Verhey, L. (2001). Horizontale werking van grondrechten in het bijzonder van het recht op privacy. Zwolle: Tjeenk Willink. p. 193.
[12] Hickey, A. (2002). Between Two Spheres: Comparing State and Federal Approaches to the Right to Privacy and Prohibitions Against Sodomy. *111 YALE L. J. 993, 994 n. 8*; and Rubenfeld. J. (1989). The Right of Privacy. *102 HARV. L. REV. 737, 749*.

Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, describing both personal information as data, afforded protection at every step, from collection to storage and dissemination.

2.2.1.- European Primary Law

At an EU level, the European Community (EC) Treaty[13] referred to data protection only indirectly in its Article 286, according to which *"Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty."*

The express recognition of the data protection right was made by the Treaty for the Functioning of the European Union (TFEU)[14] in its Article 16 (*"Everyone has the right to the protection of personal data concerning them").*

Besides, participation of the EU in the European Convention of Human Rights (ECHR)[15] and making the Charter of Fundamental Rights (Charter) legally binding primary law (in a slightly modified form)[16] in December 2009, with the entry into force of the Lisbon Treaty[17], have reinforced the protection of personal data; more precisely, Articles 7 ("*Everyone has the right to respect for his or her private and family life, home and communications*") and 8 (*"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."*) of the Charter provide for a right to privacy and a separate right to data protection,

[13] Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and related acts. Official Journal C 340, 10 November 1997.
[14] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, Official Journal of the European Union C 306, 17.12.2007, 1-271.
[15] The right to privacy is set out in Article 8 of the ECHR and data protection has been recognized as one facet of privacy by the jurisprudence of the European Court of Human Rights (ECtHR).
[16] Charter of Fundamental Rights of the European Union, Official Journal of the European Union C 83, 30.3.2010, 389-403.
[17] Supra note 14.

while Article 52(3) obliges the ECJ to abide by the content of the ECHR and furtherly the jurisprudence of the European Court of Human Rights (ECtHR), when relevant[18].

Until that time, only few Member States recognized in their legal orders a right with such a content and the European Court of Human Rights had been providing judicial protection against the unlawful processing of data in the name the right to respect private life, as established by Article 8 of the ECHR, and as developed in 1981 by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108')[19].

2.2.2.- European secondary law

The definition of personal data in the EU was made by the enactment of the Personal Data Directive[20], according to which personal data refers to *"any information relating to an identified or identifiable natural person ("data subject")",* where an identifiable person is *"one who can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*

According to Article 29 Working Party, which brings together representatives of European Data Protection Authorities, the "information" mentioned in the Data Protection Directive might relate either to objective or subjective information and might be kept in any form to be relevant for the Directive[21]. It may relate to a person either qua "content", such as medical records or qua "purpose", if it is used to evaluate or influence personal behavior or qua "result", if the consequence is that a person might be treated or looked upon differently[22]. Personal data may either be directly identifiable, such as a name, or indirectly, such as a telephone number[23].

[18] *The implications of Copyright Infringement on the Right to Data Protection in European Union law in the context of Peer-to-Peer Technology.* New Technologies and the Right to Privacy. Retrieved from http://www.nottingham.ac.uk/hrlc/documents/studentconference2010/orlalynkseyhrlcsubmission.pdf.
[19] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108.
[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**.** *Official Journal L 281 , 23/11/1995 P. 0031 - 0050,* Article 2(a).
[21] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136). 20 June 2007.
[22] Idem, p. 10.
[23] Idem, p. 12-13.

To determine whether a person is identifiable, all the means likely reasonably to be used either by the controller or by any other person to identify a person should be taken into account[24], even though such an interpretation might seem narrow, as it overlooks the "indirect" information.

Furthermore, the Data Protection Directive sets out the general principles which must be applied to data processing in order to make it lawful. The concept of data processing is defined very broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[25] In short, almost everything that can be done with personal data falls within this definition

The E-Privacy Directive[26] complements this general Directive by setting out specific rules to address data protection issues arising with regard to new technologies and electronic communications, interpreted in the light of the Charter's human rights framework, as a result of its binding provisions; more precisely, in its second recital it states that "*In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter*".

However, even after the enactement of the EU primary and secondary legislation the right to personal data protection was still an emerging right, waiting for the EU Court of Justice (ECJ), as the ultimate interpreter of EU law, to clearly define it and describe its exact content.

Actually, the ECJ proved to be reluctant to keep up with the evolution of personal data protection right. It was only in 2008 that the Court acknowledged in the Promusicae judgment[27] that *"Article 8 of the Charter expressly proclaims the right to protection of personal data".* [28] Despite that important innovation, the rest of the judgment insisted on adopting the until then used right to respect of private life.

[24] Supra note 20, Recital 26.
[25] Supra note 20, Article 2(b).
[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.
[27] Judgment of the Court (Grand Chamber), 29 January 2008, Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU.
[28] Supra note 27, § 64.

Even after the Promusicae ruling, ECJ is still not making an excessive use of the EU fundamental right to personal data protection; nonetheless, there have been instances in which the Court has made further mention of the EU right to personal data protection ("Deutsche Telekom 2011 ruling").[29]

2.3.- Personal Data in the digital era

Individuals' lives have been thoroughly affected by innovations and breakthroughs achieved especially in the field of information and communications technologies. The evolution, commercialization and accessibility of a significantly large number of people to the internet were the elements with the greatest impact. However, technology hasn't solely changed over the past 40 years, as behavior of individuals, as users of technology, has changed too.

2.3.1.- The Internet

The development of the hardware underlying informational technology has led to the acceleration of processor speed, to new techniques for the compressing of data and to the increase of memory sizes and disk storage capacity, allowing data to be collected, stored and analyzed massively, creating huge collections of data, capturing information of value to business, science, government and society. For example, search engine companies, such as Google, Yahoo!, and Microsoft, have created an entirely new business by capturing the information freely available on the World Wide Web and making it available to everyone. These companies collect trillions of bytes of data every day and continually add new services, such as satellite images, driving directions and image retrieval. The societal benefits of these services are immeasurable, having transformed how people find and make use of information on a daily basis. However, all this information accessible to anyone is being used uncontrollably.

Other important technological achievements affecting data are identically the increase of available networking bandwidth, which has permitted the transmission of

[29] Judgment of the Court (Third Chamber), 5 May 2011, Case C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland.

large amounts of data even in real time, especially in the form of audio or video streams, the development of miniaturized sensors and batteries, facilitating the excessive use and deployment in a number of different social settings and the amelioration of the sensing abilities and flexibility of such devices.

2.3.1.1.- Behavioral targeting

Increasingly sophisticated techniques ("tracking software") for collecting and analyzing personal information from multiple and disparate sources have been developed, available to individuals, companies and governments for a variety of purposes, such as routine use by governmental institutions, surveillance by public authorities and especially behavioral targeting based on consumer profiling and matching of personal data by online advertising companies.

Behavioral targeting is a technique used by online publishers, advertisers and e-commerce sites, intending to increase the effectiveness of their campaigns, through information collected on an individual's Web-browsing behavior, such as the pages they have visited on a certain date and time, the searches they have made and their purchase history, all of them kept as a record concerning the identity of the Internet Protocol (IP) address holder, in order to select which advertisements to display to that individual. This process by which an individual's profile is constructed, transforming data into knowledge, is known as "*online behavioural profiling*" and the data collection process is called "*behavioural tracking*", e.g. Facebook tracks across sites via its "Like" button, Twitter via "Tweet" button etc., providing information, even if the user does not click on this button, just by the mere view of a website containing such a button, despite his/her participation in the social network or not, as long as he or she has visited it at least once. [30]

This practice suggests that companies increase routinely their revenues by providing customized-personalized services to their customers, coming from records collected from profiling, concerning age, gender, user's interests etc.; it is obvious that these records, relying heavily on users' personal information, collected often

[30] Castelluccia, C. & Narayana, A. (2012). Privacy considerations of online behavioural tracking. *European Network and Information Security Agency (ENISA).* Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking/at_download/fullReport.

without their consent or even awareness of the processes, prospective of use and identity of myriad of actors involved, constitute a form of identification, threatening privacy, transparency and individual choice and making the possibility of the creation of a surveillance society or internet, where all online or physical activities are recorded and correlated, visible. It is not decisive whether a name can be added or not to a profile. It suffices that data can lead to identification of a person as personal data[31], as they can be used to "single out" one individual within a group[32].

It can be argued, though, that behavioral targeting could also be proved beneficial to users, who receive useful commercial and non-commercial information in line with their interests.

2.3.1.2- Web analytics

Tracking is also conducted by E-commerce companies and other website publishers, which often use fine systems for various types of aggregate measurements, such as website traffic statistics, effective exposure of advertising, the way visitors came to the site (i.e., if they followed a link or directly), what keywords they searched for on the site's search engine, how long they stayed on a given page or on the entire site, what links they clicked on and when they left the site, etc., in order to obtain aggregate traffic statistics, such as most visited pages, visitors' countries, the popularity of a website's areas etc., which measure the effectiveness of ad campaigns and evaluate their content.

Again, data is stripped of personal identifiers, such as individual names and social security numbers[33], permitting data processing, while avoiding personal information abuse.

However, behavioural targeting companies may collect anonymous data but then overlay it with other data-bases, in an attempt to bring the users' identity into

[31] Bygrave 2002, p 318; Korff 2010, p 53; Article 29 Working Party, Opinion 2/2010 on online behavioural advertising (WP 171). 22 June 2010, p 9; Opinion 4/2007 on the concept of personal data (WP 136). 20 June 2007, p 12-21.

[32] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising (WP 171). 22 June 2010, para 3.2.2.

[33] Greely, H. T. (2007). The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks. *8 Annual Review of Genomics and Human Genetics 343.*

clearer focus[34]. As Paul Ohm recently observed, "*clever adversaries can often re-identify or de-anonymize the people hidden in an anonymized database...Re-identification science disrupts the privacy policy land- scape by undermining the faith that we have placed in anonymization.*"[35]

2.3.1.3.- Cloud computing

It is a common practice for individuals and enterprises to store and process data on remotely located computers accessible through the internet rather than on local computers, such as e-mails, messaging and photo sharing services, desktops, account and finance services, payroll, customers' billing, customer relationship management (CRM), enterprise resource planning (ERP) software, computing platforms and infrastructure offerings, etc., all of them forming "*cloud services*".

"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".*[36]

This principally new business model allows the location-independent access to computer resources, that are quickly and seamlessly allocated or released in response to demand and the simultaneous processing of data distributed automatically over massively parallel hardware, succeeding reduced cost, convenient sharing of data, enhanced ability of collaboration, and increased reliability, raising, however, at the same time serious concerns regarding privacy and law enforcement access; by the storage, processing and transfer to the cloud, data changes hands from the immediate personal controller's to the record keeper's, crosses borders and may be accessed and used, read, copied and published without the knowledge and meaningful consent of individuals[37], threatening confidentiality of the information, data protection and data

[34] Tene, O. (2011). Privacy: The New Generations. *International Data Privacy Law 1 (1): 15-27, first published online October 5, 2010.*

[35] Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, Vol. 57, p. 1701.*

[36] Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145*.

[37] Robison, W. (2010). Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act. *Georgetown Law Journal, Vol. 98, No. 4, 2010*.

security and as data centers can be established in countries that provide little or no protection to personal data, running the risk of no possibility of enforcement.

2.3.2.- Mobile data processing

A growing variety of computing devices, such as mobile phones, smart phones, notebooks, laptops, portable gaming devices have become the principle tools for internet access; however, their use raises serious questions about privacy.

2.3.2.1.- Location tracking

Mobile devices containing location tracking technologies, such as the Global Position System (GPS), triangulation by cell phone towers, wireless positioning and IP location facilitate everyday life and communications by giving directions for reaching to a certain location, locating nearby friends, finding recommended restaurants in foreign cities, "checking in" at venues to receive discounts and coupons and obtaining up-to-date traffic reports[38].

However, these technological advances present unprecedented opportunities for monitoring individuals' movement[39], not always with the user's approval or awareness.

Although, the EU Directive on Privacy and Electronic Communications requires subscribers' opt-in consent for the collection and use of location data for the provision of value added services[40], yet, the ubiquity of location data collection and the indispensable use of mobile devices render ineffective the existing notice and choice regime.

It is, thus, obvious that new rules should be adopted regarding the collection[41] and process of data collected in this way as well as third party access thereto.

[38] Supra note 34.
[39] Warrior, J., McHenry, E., & McGee, K. (2003). They Know Where You Are. *IEEE Spectrum, vol. 40 no. 7, pp. 20-25.*
[40] Supra note 26; see Article 29 Data Protection Working Party, "Opinion on the use of location data with a view to providing value-added services" (WP115), 25 November 2005. Retrieved from http://ec.europa.eu/justice_home/fsj/ privacy/docs/wpdocs/2005/wp115_en.pdf.
[41] Center for Democracy & Technology Policy Post. (2009). *The Dawn of the Location-Enabled Web.* Retrieved from http://www.cdt. org/policy/dawn-location-enabled-web.; Electronic Frontier

2.3.2.2.- Third party applications

Another tool constituting a rich source of online privacy controversy[42] related to mobile data processing is third party applications (apps).

They are programs written to work within a given operating system by individuals or companies other than the provider of that operating system[43], making the life of their users more functional.

The user is often asked to give his permission to the app for access to his personal information; otherwise, the app typically cannot be used. The content of consent regards collecting, processing and sharing with advertising companies of information concerning business, education, entertainment, family, games, lifestyle, sports and utilities of users and their friends.

However, in many cases the scope, terms and consequences of information sharing are highly technical, vague and written in a dense legalese, preventing them from being readily transparent to an average user, who does not truly understand, let alone realize the risks of apps maliciously harvesting profile information.

Besides, anything shared with a third-party app is not being deleted, once the app is not used any more.

2.3.3.- The Internet of Things

Another innovation of the digital era is the emerging global Internet-based information architecture transforming everyday physical things into smart objects that can communicate with each other, understand and react to their environment, to create the so-called "internet of things".

The internet of things has various positive effects, such as the reduction in waste of time, loss and cost, the improvement of forecasting and planning, the provision of more accurate information, etc.

Foundation. (2009). *On Locational Privacy, and How to Avoid Losing it Forever*. Retrieved from http://www.eff.org/files/eff-locational- privacy.pdf.

[42] Dixon, P. & Gellman, R. (2011). *Online Privacy: A Reference Handbook*. Santa Barbara, California: ABC-CLIO, LLC.

[43] Supra note 34.

However, the collection and storage of data may lead to the creation of detailed user profiles, challenging privacy and personal data protection.

2.3.4.- Online Medical Privacy Issues

During the digital era, many kinds of health activities related to the disclosure and maintenance of personal health information, either as a medical data or as an object of medical research, take place online, offering speed, accuracy, consistency and effectiveness, contrary to the traditional practices.

Nevertheless, medical and genetic information stored online, questions posed or participation in discussions by individuals on health websites, apps assessing user's weight, mental health, etc., searches in online search engines may menace privacy; none of this information shared online by users is subject to privacy protections and, even if an individual is not identifiable to other users, the website may know who he or she is[44], having potential implications for discriminatory practices in employment, insurance and relations between citizen and state[45].

2.3.5.- New users' attitude

Apart from the technological changes which occurred during the digital age and affected data protection, there has been a radical change in the users' behavior.

Their absolute familiarization with technology, the easy access to new technologies by everyone and the dependence of everyday life, business, health, communication, etc. by online services, all these have created a new users' attitude.

They post and search for personal, even intimate, information online; they communicate with friends, partners and customers via e-mails; they expose their preferences, habits, professional skills, political, ideological and artistic tastes, social relationships, sexual interests, video and pictures of themselves in social networks; they are accustomed to publicizing their location or even having their location tracked

[44] Supra note 42.
[45] Supra note 34.

and broadcast, in search of nearby friends or restaurants; behaviors, resulting in extinguishing the borderline between private and public sphere of life.

As Professor Charles Fried had noticed from the early 70s, people are becoming more willing to reveal information about themselves, adjusting their behavior and conception to the evolution of technology[46].

However, all this sharing of data may prove to be detrimental to user's privacy and reputation; there are examples of people who lost their jobs, college admissions or relationships due to the posting of photos on social media[47].

2.3.6.- E-governance

As web technologies have developed from the pure information-sharing phase to interactive, transactional and intelligent phases, many states and countries adopted these technologies, in order to offer web-based government (e-government) services for improving government efficiency, transparency and competitiveness in the global economy.

The benefits are numerous: easy access, no waste of money and time, improved quality of information supply, reduced work-process time, fewer administrative burdens, reduced operational costs, simplification of government, improved service level, increased work efficiency and increased customer satisfaction[48].

Despite the impressive growth in the development of e-government services, serious concerns about privacy are being expressed; the e-government sites are vulnerable to cyber attackers and terrorists, which may harm not properly secured sites; citizens' names, social security numbers, property tax records or other private information may be posted on relative sites without any password protection, permitting the construction of a detailed profile of an individual, using only publicly available, individually identifiable information from government records[49].

[46] Various Staff Writers. (1970, July 27). Is privacy dead? *Newsweek Magazine*

[47] Goldberg, S. (2010, March 29). Young job-seekers hiding their Facebook pages. *CNN*. Retrieved from http://edition.cnn.com/2010/TECH/ 03/29/facebook.job-seekers/index.html.

[48] Chevallerau, F. (2005). The impact of e-government on competitiveness, growth, and jobs. *The IDABC eGovernment Observatory of European Communities.* Retrieved, from http://europa.eu.int/idabc/egovo.

[49] Bhattacharya, J. (2008). *Privacy Technology for E-Governance.* Retrieved from *www.iceg.net/2008/books/.../13_114-124....*

2.4.- IP addresses as personal data

One of the most controversial issues, not free of practical implications, is whether Internet Protocol (IP) addresses constitute personal data[50] and, consequently, if they are subject to data protection legislation.

The IP address is the unique numerical label of a device attached to an IP network, contrary to IP addresses within a local network which use the same private addresses[51], thus they are considered to be the personal trace of an individual in the online world, permitting his or her identification.

The significance of the recognition of an IP address as personal data lies in the imposition of restrictions and limitations when processing it, e.g. prior consent.

The definition of personal data provided by Directive 95/46/ EC, as abovementioned, is extremely broad, not offering a straightforward answer.

To the same direction leads Peter Fleisher's, Google Global Privacy Counsel, aspect that "*there is no black or white answer: sometimes an IP address can be considered as personal data and sometimes not, it depends on the context, and which personal information it reveals*"[52].

In this search, it is not meaningless that IP addresses identify computers and not persons, which creates uncertainty concerning the identity of the user of the computer.

According to a recent study conducted for the European Commission, IP addresses in Europe are generally considered by national authorities and courts to be personal data[53].

Similar broad interpretation of the concept of personal data in relation to IP addresses have already been adopted by the Article 29 Working Party, in former

[50] Tridimas, T. (2006). *The General Principles of EU Law*, 2nd ed. New York: Oxford University Press.
[51] PC Magazine. Retrieved from http://www.pcmag.com/encyclopedia.
[52] Sachoff, M. (Jan. 22, 2008). EU Wants IP Addresses To Be Personal. *WEBPRONEWS*. Retrieved from http://www.webpronews.com/topnews/2008/01/22/eu-wants-ip-addresses-to-be- personal.
[53] Hunton & Williams, Kuner, C., Burton C., Hladjk, J., Proust, O., Manak A., Högberg A. C. (November 2009). *Study on Online Copyright Enforcement and Data Protection in Selected Member States.* DG Internal Market of the European Commission. Retrieved from http://ec.europa.eu/internal_market/iprenforcement/ docs/study-online- enforcement_en.pdf.

opinions[54], by the European Data Protection Supervisor[55] and by Advocate General Kokott[56].

This prevailing aspect has been also followed by the Austrian doctrine and jurisprudence, as well as some Data Protection Authorities; for instance, the Belgian Privacy Commission since 2001[57], the Spanish authority since 2003[58] and the Greek authority since 2010[59].

On the contrary, some French jurisprudence[60] has followed a strict interpretation of the concept, going however against the position of the CNIL and the recently modified French Data Protection Act.

[54] Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, WP58, 30 May 2001 and Opinion 2/2007 on the concept of personal data, WP 136, 20 June 2007.
[55] Opinion of the EDPS of 22 February 2010 on the current negotiations by the European Union of an Anti- Counterfeiting Trade Agreement (ACTA), 2010/C 147/01, paras 25-28.
[56] Opinion of Advocate General Kokott, C-274/06 Productores de Musica de Espana v Telefonica de Espana SAU, delivered on 18 July 2007, paras 61-62.
[57] Commission de la Protection de la Vie Privée, Opinion n°44/2001 on the compatibility of detection of copyright infractions on the Internet with the legal provisions relative to data protection and telecom- munications [d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications].
[58] Agencia Española de Protección de Datos, Legal Opinion 327/2003, IP addresses as personal data [Carácter de dato personal de la dirección IP].
[59] Greek Data Protection Authority-Consultation Documents of 12.04.2010 and 02.08.2010.
[60] Appeal Court of Paris, 13th Ch., sect. B, 27 April 2007, Guillemot et C.A. Paris, 13th Ch. Sect. A, 15 May 2007, Sebaux and D C n°2004-499 of 29 July 2004.

3. INTELLECTUAL PROTPERTY IN THE DIGITAL AGE

3.1.- Historical background

Intellectual property regulates the creation, use and exploitation of mental or creative labor in the industrial, scientific, literary and artistic fields.

Although the human desire to claim for property rights is inherent even since the infancy, the legal recognition of property in the ideas is a relatively recent phenomenon; actually, it was officially recognized much later than the official recognition of property rights in tangible and intangible objects.

The primary attempts for safeguarding the property over certain practices and ideas were made after the invention of writing; however, the disputes were very limited, as manual unauthorized copying of entire works was too laborious for piracy to be profitable.

The invention of movable-type printing offered the ability of a fast and easy reproduction of multiple works, facilitating the unauthorized copying and making the demand for a monopoly control of the "owners" over their own works and practices more intense. It was during the Renaissance that the three best-known forms of intellectual property appeared in Europe: copyright, referring to the protection of expressive works; trademark, referring to the distinction of goods by identifying the marker or distributor; and patent, referring to the protection of inventions.

However, the information technology revolution taking place right now has thoroughly affected the intellectual property rights due to the possibilities given to anyone by personal computing and internet; much web content borrows and incorporates existing material and the extent to which such borrowing should be permitted has not yet been fully resolved and many users create no content of their own, but merely make and pass along unauthorized copies of existing content[61]. It is

[61] Schwabach, A. (2007). *Intellectual Property: a Reference Handbook.* Santa Barbara, California: ABC-CLIO, Inc.

obvious that the most affected by the digital revolution form of intellectual property is copyright.

3.2.- Copyright

Copyright is as set of exclusive and intangible rights granted to the author of a creative work, protecting and enabling his/her control over his/her creation.

As a property right, copyright is protected under Article 17 of the Charter of Fundamental Rights of the European Union and by the European Convention on Human Rights and Fundamental Freedoms, combined with Article 1 of the First Additional Protocol to the ECHR,[62] according to which *"every natural or legal person is entitled to the peaceful enjoyment of his possessions and no one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law"*.

There was no substantive legal provision concerning the protection of any of the intellectual property rights in The European Community (EC) Treaty.

Nevertheless, the Treaty for the Functioning of the European Union (TFEU)[63] recognized explicitly the intellectual property rights in its Article 118 (*"In the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralized Union-wide authorization, coordination and supervision arrangements").*

Furthermore, pursuant to Article 2(a) of the Information Society Directive[64], Member States have the obligation to provide for the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in

[62] Geiger, C. (2009). Intellectual property shall be protected!? Article 17(2) of the Charter of Fundamental Rights of the European Union: a Mysterious Provision with an Unclear Scope. *European intellectual property review, 31*(3), p.117; ECtHR Case Balan v Moldova, January 24, 2012; Judgment of the Court (Grand Chamber) of 3 September 2008, joined cases C-402/05 P & C- 415/05, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, para.356.

[63] Supra note 14.

[64] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society. (OJ L 167 of 22.06.2001).

any form, in whole or in part, for authors, of their works, on the basis that an author's work is an extension of his/her personality, therefore he/she should have control over it ("moral right") and that the author should reap the economic benefits of his work ("economic right"). Absent a protective regime, the authors would have no economic incentive to create[65], setting under risk the whole creative industry.

There is, additionally, a variety of secondary legislation setting the legal framework of copyright protection; identically, the E- commerce Directive[66] and the IPRs enforcement Directive[67], all of them interpreted in the light of the Charter's human rights framework, as a result of its binding provisions.

3.3.- Copyright in the digital age

Serious concerns are raised the last years about copyright; globalization, digitization of media, rapid expansion of the internet and increasing popularity of "MP3" audio compression have reduced the cost of transportation and communication across the world[68], have facilitated and increased the quick flow of copyrightable works[69] perfectly, cheaply and anonymously, have allowed cross-border transfer of digital works in seconds, and have decreased the costs of data bandwidth and storage, while at the same time prosecution and punishment became so much more remote.

These trends have seriously affected the control of copyright owners concerning the way content gets to consumers, contrary to the existing business models, which were relying on controlled distribution and broadcast channels. Thus, in the past, copyright was not a major threat, as long as illegal copies were expensive to make, of drastically inferior quality, or, at least, limited in scale[70].

Most concerned with this new situation is by far the entertainment industry, as ordinary people forming until then the "audience" can now generate, copy, modify

[65] Cruz, L. The Copyright Industries and the challenges of protecting Intellectual Property in the digital age. *Academia. edu.* Retrieved from https://www.academia.edu/3676219/The_Copyright_Industries_and_the_challenges_of_protecting_Intellectual_Property_in_the_digital_age.

[66] Directive 2000/31/EC (Directive on certain legal aspects of electronic commerce in the Internal Market, commonly known as the "E-Commerce Directive"). (OJ L178 of 17.07.2000).

[67] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Official Journal L 157 of 30.4.2004).

[68] Stiglitz, J. (2002). *Globalization and its Discontents*. New York: W.W. Norton & Company, Inc.

[69] Negroponte, N. (1995). *Being Digital*. London: Hodder and Stoughton, Ltd.

[70] Belleflamme, P. & Peitz, M. (2010). Digital Piracy: Theory. *CESIFO Working Paper No. 3222*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1698618.

and share works with a global public, without having to deal with commercial content intermediaries, such as publishers, record labels or studios[71].

Furthermore, copyright law is unable to keep up with social developments or adapt to the digital age, following and comprehending the technological breakthroughs, in order to regulate newly established unlawful behaviors. The result is the enactment of too rigid, inflexible, vague and outdated by the time of their publication legislative measures, acting as an obstacle to innovation and to citizens' access and use of their own culture, while online infringers are always one step ahead of right holders and legislators[72].

Even the sanctions, which may be provided in copyright law, are unable to prevent infringement, as, even if infringers are aware of breaking the law, they perceive as very remote the sanctions that they may encounter, in case they are caught buying or making copies.

3.3.1.- Digital Piracy

The most alarming form of copyright infringement is digital piracy, regarding the unauthorized copying and distribution of copyrighted material via electronic means, e.g. streaming a video from an illegal site or downloading a file without paying for it. The objects of digital piracy may include everything which can be distributed over the internet, ranging from TV shows and movies to games, software, e-books and music[73].

What constitutes digital piracy so complicated is the possibility of sharing illegal content with billions of people across a worldwide network instantly, just by clicking a button, the absence of any physical trace of the offender, the differentiation of legislations from country to country concerning what is legal or not, while at the same time the internet allows for cross-border activities, as well as the fact that all free downloads are not necessarily legal and all paid downloads are not necessarily legitimate.

[71] Bollier, D. (2011). *Intellectual Property in the Digital Age*. Chapter 5 from Ben Walmsley, *Key Issues in the Arts and Entertainment Industry*. Oxford, England: Goodfellows Publishers Ltd.

[72] Morris, P. S. (2009). Pirates of the Internet at Intellectual Property's End with Torrents and challenges for choice of law. International Journal of Law & Information Technology, 17(3), 282-303, p. 283.

[73] Meyer, S. (2013). *Understanding Digital Piracy*. New York: The Rosen Publishing Group, Inc.

Many different industries suffer big losses due to digital piracy, as consumer prefers the download option instead of effecting a purchase; as a consequence, at best, profits remain unchanged or, more realistically, they get reduced, with further implications to the loss of jobs in industry and to the nations' economies. All piracy is detrimental to the very substance of copyright, as well as to the interests of the right holder.

Furthermore, even if the copyright holder receives an adequate remuneration for the user's private use, still online private copies' sharing cannot possibly be regarded as personal use and legitimate exploitation of the work[74]. Piracy limits the monopoly power of the supplier of the original.

Nevertheless, there some who assert that illegal downloading of e.g. music files has a positive effect on sales in digital format[75], as it offers the possibility to sample the product prior to purchase and that uncontrollable downloading may prove beneficial to the sales of less popular films, acting as a mechanism to spread information[76].

3.3.2.- Peer-to-peer file-sharing

The most common type of digital piracy is the use of online peer-to-peer networks that facilitate the swapping of music and video files between users.

Peer-to-peer (P2P) is a technology that creates networks of internet users allowing them to easily communicate with each other and share content files and information, such as music and video files, often without the intellectual property rights owners' approval[77]. This procedure takes place either directly from one computer (peer) to another or through a mediating server via the internet, without control of the flow of information circulating among peers by a "central" server. Each

[74] Kisieliute, I. (2012). *A "fair balance" between intellectual property rights and other fundamental rights?* (University essay). Lund University, Sweden.

[75] Aguiar, L. & Martens, B. (2013). Digital Music Consumption on the Internet: Evidence from Clickstream Data. *European Commission Joint Research Centre Institute for Prospective Technological Studies Luxembourg: Publications Office of the European Union*.

[76] Peukert, C., Claussen, J., Kretschmer, T. (2013). Piracy and Movie Revenues: Evidence from Megaupload: A Tale of the Long Tail? *Social Science Research Network (SSRN)*. Retrieved from http://ssrn.com/abstract=2176246 or http://dx.doi.org/10.2139/ssrn.2176246.

[77] Wright, T., Liotta, A., Hodgkinson, D. (2008). E-privacy and copyright in online content distribution: a European overview. *World Data Protection Report. BNA International. Volume 8, Number 5*.

computer works both as a client (information requester) and a server (information provider), leading online piracy to reach unprecedented levels.

The beginning was made in 1999 by the first popular online P2P file-sharing network, Napster, which used a centralized server acting as a search engine to assist users to download music compressed in an MP3 format from the computers of other Napster subscribers. Napster became the fastest growing application in the internet's history, expanding to include approximately 25 million users within its first 12 months of operation[78].

Nevertheless, Courts found the provider of this system liable for copyright infringement[79], leading to the emergence of second and third generation P2P file-sharing networks, such as Gnutella, Kazaa, BitTorrent and Pirate Bay, which were highly decentralized and liability was difficult to be proved[80].

In 2002 it was estimated that 99% of all files transferred through such P2P systems were unauthorized[81]; this consumer tendency has led to the reduction of worldwide revenues, coming from entertainment industries.

However, there also some opposite opinions, asserting that P2P file-sharing's utility may also be found in the fact that it allows users to distribute their own creations for free, if they wish, and that it provides works that are either no longer available or have long fallen into public domain and therefore, can be legally shared as there is no copyright to be infringed[82].

3.4.- ISPs' liability

Due to the increasing phenomenon of copyright infringement attributed mostly to file-sharing programs over the internet, copyright industries indicated technical intermediaries' and more precisely Internet Service Providers' (ISPs) liability as the

[78] Lim, D. (2007). Beyond Microsoft: Intellectual Property, Peer Production and the Law's Concern with Market Dominance. *Fordham Intellectual Property, Media And Entertainment. Law Journal.* Vol. 18, Iss. 2.
[79] e.g., see A&M RECORDS, Inc. v. NAPSTER, INC., 239 F.3d 1004 (9th Cir. 2001).
[80] Johnson, M. E., McGuire, D., Willey, N. D. (2008). The Evolution of the Peer-to-Peer File-Sharing Industry and the Security Risks for Users. *Proceedings of the 41st Hawaii International Conference on System Sciences*. Retrieved from http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/publications/pdf/30750383_1.pdf.
[81] World Intellectual Property Organization. *The Impact of the Internet on Intellectual Property Law.* Retrieved from http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap3.html.
[82] Lessig, L. (2004). *Free Culture: How Big Media uses technology and the Law to lock down culture and control creativity.* New York: The Penguin Press.

key to combating it, on the grounds that P2P users are often difficult to get identified and located, whereas ISPs constitute an attractive target for legal action, as they are visible, well known, and their financial strength is likely to be greater than that of their customers or users[83].

An ISP is a company or other organization that provides access to the internet, usually against payment, enabling users to establish contact with the public network. Many of them also provide e-mail services, storage capacity, proprietary chat rooms, games and information to their subscribers.

The first European case which had to deal with the issue of intermediary liability was the 1999 Godfrey v. Demon case regarding defamation, where the English Court ruled that the UK ISP could be liable under English defamation law, as it had failed to comply with the plaintiff's request to remove offensive postings from one of its newsgroups within the concrete time limit and therefore it contributed to the publication of the defamatory statement.[84]

In the Community level, the issue of the ISP liability was regulated by the E-commerce Directive[85], which followed a horizontal approach, imposing the same regime to any type of infringement regardless of the area of law, e.g. copyright, defamation, privacy rights, etc., whereas the application of a strict liability regime different for the various areas of law would impair the expansion of electronic commerce within the EU[86],

The Directive provides for a system of specific liability exemptions; when an ISP serves as a "mere conduit", meaning that the ISP is acting as a provider of internet access[87]; when ISP provides "temporary caching", meaning automatic, intermediate and temporary storage of data in local servers, so long as it does not modify the information and it complies with conditions on access to the information[88].

Hosting services are also exempted from ISPs' liability, so long as ISPs are "*not aware of facts or circumstances from which the illegal activity or information is apparent*" (when it concerns civil claims for damages) or they "*do not have actual knowledge of illegal activity or information*" (when it concerns other claims) and so

[83] Lloyd, I. J. (2008). *Information Technology Law*. New York: Oxford University Press.
[84] Godfrey v. Demon Internet Ltd., [1999] 4 All E.R. 342 (Queen's Bench Division, March 26, 1999).
[85] Supra note 66.
[86] Internet Business Law Services (IBLIS). (February 21, 2008). Editorial Board, *Internet Law - How does the European Union Treat Copyrights?*
[87] Article 12 E-Commerce Directive, supra note 66.
[88] Article 13 E-Commerce Directive, supra note 66.

long as they act "*expeditiously*" to remove or block access to an information with an unlawful nature, once they get aware of it[89].

Moreover, the Directive does not impose any general monitoring obligation to ISPs concerning the data they transmit or store nor a general obligation to seek actively facts or circumstances that would indicate illegal activity. However, national courts or administrative authorities are allowed to impose a relevant obligation limited to specific and clearly defined individual cases[90].

The rationale behind this regulation is that ISPs, similarly to a telephone carrier, provide communication services; therefore, they cannot be held liable for the content of the communication. Additionally, this would be impossible for large ISPs which host daily millions of posts.

In a different case where content policing would be obligatory for ISPs, the subscriber costs would surely be much higher, resulting in the exclusion of an excessive number of users from access to cyberspace.

However, right holders insist that the EU regime is outdated and therefore, prevents them from effectively protecting their rights on the internet. The answer of the ECJ in its Promusicae[91] and Scarlet[92] judgments referring to Article 15 of the E-Commerce Directive can be interpreted as a confirmation that the neutrality principle regarding ISPs liability should stay untouched.

3.5.- Digital Rights Management

Digital Rights Management (DRM) is a collection of systems used by copyright holders all around the world to protect copyright on electronic media, such as digital music and films, as well as computer software, by controlling the user's ability to access, copy, print, transfer and convert material.

Advisory DRM labels the media as protected and authorized players refuse to copy such protected material, while DRM containing encryption schemes permits only specific software to unlock it, without legal enforcement, just by a certain format

[89] Article 14 E-Commerce Directive, supra note 66.
[90] Article 15 E-Commerce Directive, supra note 66.
[91] Supra note 27.
[92] Judgment of the Court (Third Chamber), 24 November 2011, Case C-70/10, Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

provided by the media companies or it can be linked to a specific type of device, for instance, video games to special consoles[93].

The Information Society Directive forbids the circumvention of "effective" DRM technologies.

The defenders of DRM allege that its significance lies in guaranteeing the appropriate right holders' revenue for their products and in limiting the unauthorized reuse of copyright works.

On the opposite side stand those who argue, highlighting that the problem still exists, as DRM's imposed restrictions on legally acquired content, increase incentives for illegal accessing content.

Furthermore, they consider DRM as a hurdle against development, especially regarding developing countries' access to knowledge and information[94] and as a means of increasing the copyright holders' power imposing unilaterally their "terms and conditions"[95], to the detriment of consumers' rights, whose right of private use is getting limited, exceeding their reasonable expectations created from the fact that they have paid for the product.

DRM's controversial nature is also proved by the fact that it gives content providers control over the digital files bought by the users; it is characteristic that a few years ago, Amazon remotely deleted digital copy of George Orwell's 1984 from users Kindle devices after a copyright clearance mistake[96].

[93] Boldrin, M. & Levine, D. K. (2009). Against Intellectual Monopoly. Syracuse Science & Technology Law Reporter. Vol. 21, Art. 6.
[94] Lucchi, N. (2006). *Digital Media & Intellectual Property/ Management of Rights and Consumer Protection in a Comparative Analysis.* Germany: Springer.
[95] Ibid.
[96] Stone, B. (July 17, 2009). Amazon Erases Orwell Books from Kindle. *New York Times*. Retrieved from http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

4. THE RISING TENSIONS BETWEEN DATA PROTECTION AND INTELLECTUAL PROPERTY IN THE DIGITAL AGE

4.1.- The relation between Data Protection and Intellectual property

Both data protection right and intellectual property right have been reformed due to the technological developments that have taken place, making their interrelation very complicated. The collision between personal data and copyright, though undesirable, seems to be inevitable for the moment, since enforcing intellectual property rights online, demands some form of regulation of online traffic[97], such as identification of alleged infringers, installation of preventive measures, implementation of specific a posteriori measures etc., initiatives seemingly conflicting with individuals' fundamental rights, one of them being personal data protection.

More precisely, the enforcement of illegal downloading of protected intellectual property works, e.g. through P2P networks, presupposes the revelation by the ISPs of contact details and content of data downloaded by the end-users, concerning disclosure of identity as well as consuming preferences and interests, all of them considered to be individuals' protected personal data; and here comes the dilemma: which protected right should supersede?

4.2.- Pertinent case-law of the ECJ

The acknowledgement of the right to intellectual property as an expression of the right to property by the European Court of Justice was first made by its Laserdisken judgment[98], according to which a potential restriction on the freedom to

[97] Rantou, M. (2012). The growing tension between Copyright and Personal Data Protection on an online environment: The position of the Internet Service Providers according to the European Court of Justice. *European Journal of Law and Technology, Vol. 3, Issue 2*.

[98] Judgement of the Court (Grand Chamber), 18 September 2006, Case C-479/04, Laserdisken ApS v Kulturministeriet.

receive information as a result of the exhaustion doctrine may be *justified in the light of the need to protect intellectual property rights, including copyright, which form part of the right to property*[99].

Nevertheless, the ECJ has also consistently ruled that the right to property is not absolute, meaning that it must be viewed in relation to its social function[100].

Consequently, measures which restrict intellectual property rights, but at the same time have Community objectives of general interest that do not constitute a disproportionate and intolerable interference in relation to the aim pursued or do not impair the very substance of the right guaranteed, are deemed permissible[101].

The first important ECJ ruling regarding data protection and the internet was the Lindqvist case[102], according to which it is for Member States to not only interpret their laws in a way consistent with the Data Protection Directive, but also to make sure that they do not rely on an interpretation of the Directive that would conflict with other rights protected by the Community legal order.

In Satamedia case[103], the ECJ did not grant sufficient and explicit weight to the right to privacy vis-a-vis another ECHR right, in that case the freedom of expression and, as Article 9 of the Directive provides for derogations to the Directive when data is processed for "journalistic purposes", the Court left it to the national court's discretion to consider on the facts the existence of the concept of journalism or not, leading to a possibility of differing standards of protection of the right to privacy throughout the Union.

4.3.- The collision of intellectual property and data protection

4.3.1.- The Peppermint case

Peppermint Jam Records, a German record company, charged Logistep, a Swiss company specialized in anti-piracy software solutions, to monitor P2P

[99] Ibid., para. 65.
[100] See for instance, C- 44/79 Hauer [1979] ECR 3727; Case 5/88 Wachauf [1989] ECR 2609; Case C-280/93 Germany v Council [1994] ECR I-4973; and C- 84/95, Bosphorus Airways [1996] ECR I-3953.
[101] Supra note 66.
[102] Judgment of the Court, 6 November 2003, Case C-101/01, Bodil Lindqvist.
[103] Judgement of the Court (Grand Chamber), 16 December 2008, Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia.

networks, in order to identify Internet Protocol (IP) addresses of users who uploaded or downloaded protected works and furtherly prosecute them.

The Italian Court of first instance ordered the ISPs to undertake such disclosure, while the Court of Appeal, being in line with the Data Protection Authority's opinion, rejected such request on the basis of data protection violations.

More precisely, both Peppermint and Logistep were considered to have been unfairly processing personal data, without the awareness or consent of the data subjects to such an activity.

On the other hand, the ISPs were neither obliged nor entitled to disclose such data to third parties without the data subjects' consent unless in cases of criminal proceedings[104]. The protection of individuals' confidentiality rights superseded against copyright owners' intellectual property rights.

It is obvious that the Peppermint Court followed the former guidelines provided by the ECJ to find a "balance" among different fundamental rights.

Contrary to the Italian Court' s judgment, a Belgian court not only considered filtering technology legal, but it also ordered an ISP to adopt and implement specific filtering technology, in order to detect illegal P2P activity and block it.

4.3.2.- The Promusicae case

One of the conflicting situations brought about by the information society was dealt by the Court in the Promusicae case[105], which was the first one to be brought to Court regarding the tension between the enforcement of intellectual property owners' rights, internet users' privacy rights and the role of Internet Service Providers (ISPs) in relation to online piracy.

On November 28, 2005 Promusicae, a Spanish non- profit-making organization representing producers and publishers of musical and audiovisual recordings sought to obtain a court order in Spain against Telefonica, Spain's top telecoms operator, in order to oblige the ISP to disclose the identities and physical addresses of certain persons whom it provided with internet access, on the grounds of illegal file-sharing of copyright work via the P2P network KaZaA, the exploitation

[104] Peppermint v Telecom Italia spa, Orders of the court of Rome of 9 February 2007 (1st instance) and 14 July 2007 (appeal).
[105] Supra note 27.

rights of which (files) were held by members of Promusicae, in order to bring civil proceedings against them.

On December 21, 2005 the Madrid Commercial Court Juzgado de lo Mercantil No. 5 granted the preliminary measures requested by Promusiacae.

Telefonica appealed, arguing that communication of such data was authorized under Spanish law only for a criminal investigation or to safeguard public security and the national defense, so the Spanish Court decided to stay proceedings and refer the case to the ECJ about the contradiction of Spanish law with Community law.

The question posed was whether Community law, in particular Directives 2000/31[106], 2001/29[107] and 2004/48[108] read in the light of Articles 17 and 47 of the EUCFR, require Member States to introduce an obligation to information society service providers to communicate connection and traffic data in the context of civil proceedings[109].

The answer came by the ECJ after a three step process[110].

Firstly the Court considered whether E- Privacy Directive precludes the Member-States from introducing an obligation to communicate personal data, in order to enable right holders to bring civil proceedings against alleged infringers. The Court concluded that Directives 2002/58/EC and 95/46/EC do not preclude Member States to lay down such an obligation[111], nor do they, however, compel Member States to set forth such an obligation[112], while based on article 15 (1) of the E-Privacy Directive, personal data protection provisions could be restricted in the light of rights and freedoms of other individuals (i.e. the copyright holders)[113].

Proceeding furtherly to the second step, the ECJ had to determine whether the three copyright Directives (2000/31/EC, 2001/29/EC and 2004/48/EC) expressly demanded from the Member States to lay down an obligation to communicate personal data in the context of civil proceedings, in order to ensure effective protection of copyright. The answer was that copyright protection cannot affect the

[106] Supra note 66.
[107] Supra note 64.
[108] Supra note 67.
[109] Supra note 27, paras 34 and 41.
[110] Supra note 27, para. 46.
[111] Supra note 27, para. 55.
[112] Supra note 27, paras. 58 and 59.
[113] Hetherington, L. (2008). Peer-to-peer file-sharing – ISPs and disclosure of user identities. *Entertainment Law Review. 19(4), 81-82, p. 81.*

provisions relating to personal data protection and that there was no requirement for Member States to introduce an obligation for personal data communication.

Since the secondary legislation did not provide any clear answer on the issue at stake, the Court, in its third step, turned its attention to primary EC constitutional law, namely to the fundamental rights of property, including intellectual property rights, such as copyright, and to the right to effective judicial protection. The Court noted, however, that these rights must be balanced against the right to the protection of personal data and hence of private life[114], with mechanisms included in the E-Privacy Directive and the Copyright Directives, as well as in national legislation.

So finally, the Court reached the conclusion that there is neither an obligation nor a prohibition on Member States to compel ISPs to provide personal data to third parties in the context of civil proceedings, that Member States must simply ensure that they strike a fair balance between competing fundamental rights when applying the national laws which transpose the Directives and that they must interpret them in a manner which is not conflictive with fundamental rights and general principles of Community law[115], for instance the principle of proportionality.

4.4.- Promusicae: a compromising ruling

Initially, the ECJ's ruling in Promusicae may seem to be a defeat for right holders, while at the same time beneficial for representatives of ISPs and internet users[116], as they were not obliged to assume any commitments regarding stricter privacy legislation etc.

Nevertheless, in a more careful view, this ruling will seem as compromising; it tried to take into account the competing arguments of ISPs, right holders and users, by avoiding a straightforward reply to the question posed, leaving an "open door"[117] to Member States concerning the introduction of an obligation for disclosure of personal data when dealing with the issue of online copyright infringement. This discretion can

[114] Supranote 27, para. 63.
[115] Supranote 27, para. 68.
[116] Herman, M. (January 30, 2008). Court delivers a blow to record companies on internet piracy. The Times. Law. Retrieved from http://business.timesonline.co.uk/tol/business/law/ article3273960.ece.
[117] Kuner, C. (2008). Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice. *European Intellectual Property Review 30(5), 199-202, p. 201.*

be viewed as a weapon for national authorities and at the same time as a defense mechanism for the public, present in three different stages.

Firstly, Member States are free to introduce the necessary legislative measures, in order to regulate the issue, in the context of the EU Directives, offering general guidelines and guaranteeing the interests of the general public.

Secondly, Member States enjoy discretion when transposing the relevant Directives in their national legal order, as they must "*take care to rely on an interpretation of the Directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order*"[118] and it is their intervention that safeguards the users' rights to privacy and prohibits ISPs from becoming the 'internet's police'[119].

Finally, according to the ECJ, national authorities and courts enjoy discretion when implementing measures for transposing the relevant Directives, respecting the principle of proportionality, which constitutes the final protection mechanism safeguarding the interests of users and ISPs.

4.5.- Data protection: an autonomous fundamental right

The contribution of the abovementioned cases, and especially Promusicae, was remarkable; until then, the fundamental right to property, including intellectual property rights, such as copyright, constituted general principles of Community law[120], while it was the first time that the ECJ expressly recognized that the right that guarantees protection of personal data and hence of private life[121] enjoys the status of a fundamental right within the Community legal order, just on the grounds that protection of personal data was enshrined in the Charter[122].

4.6.- ECJ's approach: fair balance

[118] Supra note 27, para 71.
[119] Weston, M. (June 12, 2011). ISP: Internet Service Provider or internet service police? *I. P.M.*
[120] Supra note 27, para 62.
[121] Supra note 27, para 63.
[122] Akrivopoulou, C. & Psygkas, A. (2010) *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*. IGI Global.

What the ECJ actually said and the Peppermint Courts applied in the aforementioned most characteristic cases of digital collision between copyright and data protection is that Member States, though not required, are free to impose in their national law an obligation on ISPs to disclose their subscribers' personal data in a civil copyright case; however, this imposition must be proportionate and must reconcile the different protected fundamental rights, applying the fair balance doctrine, namely the protection of property, the right of privacy and furtherly the effective remedy right.

In a few words, none of these rights supersedes over the other ab initio.

4.6.1.- Fair Balance

Fundamental rights, though equal in law, are not always treated equally in practice due to various factors. The clash of fundamental rights could be compared with a "*classical philosophical opposition*", which never encounters "*peaceful coexistence*" of the two opposing concepts, but rather a "*violent hierarchy*", where one of the two dominates over the other[123].

What comes out of ECJ case law is that a fair balance has to be struck between the various fundamental rights involved when the Member States transpose secondary legislation protecting these rights and/or apply the implementing national legislation[124].

When referring to the doctrine of "fair balance" it is always a matter of assessment of different divergent and conflicting interests that must be taken into account under a certain context; while the applicable law maybe the same, the outcome in cases of balancing is directly dependant on the context.

The substance of balancing is that "*the greater the degree of non-satisfaction of, or detriment to, one principle, the greater the importance of satisfying the other"*[125]; thus, the degree of non satisfaction or of being detrimental to a first principle should be estimated initially; then, the importance of satisfying the

[123] Derrida, J. (1981). *Positions*. Chicago: The University of Chicago.
[124] Supra note 27, para.68; Court order in C-557/07 Tele2 v. LSG, para. 28; Case C-70/10 Scarlet Extended, para.45; Case C-360/10 SABAM v. Netlog, para.43; Case C-461/10 Bonnier, para.56.
[125] Alexy, R. (2013). Balancing, constitutional review, and representation. *International Journal of Constitutional Law 11(3).*

competing principle; and lastly, whether the importance of satisfying the latter principle justifies the detriment to or non-satisfaction of the former[126].

The ECJ uses fair balance in widely different areas of case-law and adopts different methods when examining the various fundamental rights, such as the teleological method, giving priority to the interpretation that gives the most effect and value to the right at stake[127].

The ECJ attempted to clarify the notion of "fair balance" in Scarlet case[128], where there was a collision of four fundamental rights, intellectual property, freedom to conduct business, personal data protection and freedom of information, stating that "IP rights are not inviolable" , in conjunction with the freedom to conduct business and the freedom of information, whereas balancing copyright against personal data protection was already dealt with in Promusicae case, both cases constituting two innovative and extremely important arguments in favor of ISPs and internet users.

4.6.2.- Proportionality

In the theoretical literature, proportionality is a legal principle regarding balancing between competing values or principles, uniquely suited to decide constitutional disputes.

Within the EU, proportionality principally serves as a framework determining, both at the EU level as well as at the level of the Member States, whether and/or to what extent rights can be limited by governmental intervention (such as legislation), motivated by public interests. One seasoned observer, Schwarze, believes the proportionality principle is the most important general principle in the field of EU economic law because in the absence of a detailed system of EU administrative law, it judges measures by the relationship between the objective pursued and the methods used[129].

Proportionality requires that measures taken should be appropriate and necessary to achieve the goal pursued, enabling, thus, judges to decide whether a

[126] Groussot, X. (2008). Rock the KaZaA*:* Another Clash of Fundamental Rights. *CMLRev*. *45*, p.1760; supra note 111.
[127] Lehrberg, B. (2006).: *Praktisk Juridisk Metod*. Uppsaa:I.B.A. Institutet för Bank- och Affärsjuridik AB.
[128] Supra note 92.
[129] Schwartze, J. (2006). *European administrative law.* Revised ed. London: Sweet & Maxwell. pp. 664-665, citing J. Gündisch and B. Schlink.

measure has gone beyond what is required to attain a legitimate goal and whether its claimed benefits exceed the costs.

Therefore, in order to reach to a conclusion whether the measure at stake is proportionate, a three-part test must be conducted, in conjunction with the three main elements forming proportionality: the "suitability test" defining whether the measure is reasonably likely to achieve the desired aim; the "necessity test" evaluating whether there are other less restrictive means capable of producing the same result; and the "proportionality stricto sensu" test, weighing the interests, in order the measure not to be excessively burdensome on an individual, in relation to the objective that is intended to be reached[130].

Both the EU intellectual property and data protection legislation have adopted the principle of proportionality. Article 8§1 of Directive 2001/29 and Article 3 of Directive 2004/49 state that measures, sanctions and remedies against infringements of intellectual property rights should not only be effective and dissuasive, but also "appropriate", "proportionate", "loyal" and "fair".

Moreover, under Article 8 of the Directive 2004/48, a Court may order the communication of information on the origin and distribution networks of the goods or services which infringe an intellectual property right, only when the request is justified and proportionate.

In data protection legislation, the principle of proportionality defines not only the processing of data, but also the adequacy and relevance of the means used for the accomplishment of these purposes in a democratic society.[131]

Furtherly, in the Lindqvist case[132], the ECJ specified that when applying the principle of proportionality, all circumstances of the case should be taken into consideration, in particular the duration of the violation of the provisions that transpose the Data Protection Directive, and the significance for data subjects of the protection of the disclosed data.

[130] Supra note 69.
[131] Coudert, F. & Werkers, E. (2008). In The Aftermath of the Promusicae Case: How to Strike the Balance? *International Journal of Law and Information Technology © Oxford University Press. Vol. 18, Issue 1 pp. 50-71.*
[132] Supra note 102.

5.- CONCLUSIONS

Until recently, the mere idea of a conflict between copyright and privacy rights, both recognized as human rights protected by the EU legislation would be quite surprising, as they have been developed autonomously in tangentially unrelated fields and hence they have co-existed peacefully. However, the advent of digital technology, especially the internet, submitted right holders to massive on-line copyright infringements, mainly through file-sharing on peer-to-peer (P2P) systems, and urged them to the development of highly intrusive new enforcement strategies in electronic communications, intending to identify the infringers and the committed infractions, involving personal electronic information of consumers of online copyrighted works. The crucial issue here was whether the damage caused to the cultural industry by the illicit exchange of protected work in P2P networks constituted a sufficient threat to copyright holders' interests, so as to justify such restrictions.

However, all sorts of private file sharing are not fair to be linked with copyright infringement, especially when they do not entail profit or commercial goal, so as to affect copyright protection to such an extent which justifies recourse to measures limiting privacy. Therefore, it would be wrong to consider file-sharers and organized pirates identical indiscriminately[133].

Things became even more complicated due to the recent constitutionalisation of the Charter of Fundamental Rights[134], which theoretically equalized all fundamental rights.

Though fundamental, nevertheless, these rights are not absolute, as they may be restricted occasionally, in order to protect the rights and freedoms of others[135], applying the Law of Balancing, which constitutes the core of a fully functioning information society[136].

This became more obvious with the Promusicae ruling, which, nevertheless, did not introduce any innovation, but it rather remained consistent with older case

[133] European Parliament Resolution on cultural industries in Europe, 10 April 2008. Retrieved from http://www.europarl.europa.eu/oeil/spdoc.do?i=14748&j=1&l=en.
[134] Art.6(1) TEU.
[135] Art.52(1) ChFR.
[136] Supra note 74.

law, stating that Member States have to respect fundamental rights when implementing Union law[137] and reconcile contradictory values[138].

In fact, the balancing process was already mentioned in the Lindqvist case[139], "*it is, rather, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved*."[140]

Moreover, the Promusicae indicated that the process of transposing secondary legislation must be conducted in a way that ensures adequate protection for all the interests in the information society; especially, when those interests are also fundamental rights, which must be weighed against each other, even though it is hard to achieve in practice.

By adopting ambiguous terms, such as the notion of "fair balance" and leaving it to the Member States to regulate the issue, the ECJ proved reluctant to impose obligations on ISPs and to restrict the freedom of internet users, avoiding "over-regulation" of the internet or taking the part of users.

The absence of any clear guidelines by the ECJ on how a fair balance is struck may, however, entail serious implications.

From one hand, the ECJ ignores that the outcome of each national court, in considering both privacy and intellectual property right, is likely to differ, according to its national constitutional culture, leading possibly to conflicting conclusions and from the other, national legislators are likely to develop different mechanisms, while seeking for effective enforcement of intellectual property rights, leading to divergent solutions.

In both cases, there is the risk of negative implications in the exercise of the fundamental freedoms of the recipients of internet (e.g. customers) and ISPs (by distorting the competition amongst them), of the coherence of the internal market, of hindering free movement of personal data within the European Union and of reaching to different standards of protection of the right to privacy throughout the Union, such as French "three - strikes" law Hadopi and UK's Digital Economy Bill.

[137] Judgment of the Court, 13 July 1989, Case 5/88, Wachauf v. Bundesamt für Ernährung und Forstwirtschaft, ECR 2609.
[138] Case C-112/00 Schmidberger para.77; Case C-36/02 Omega Spielhallen para. 36; Case C-341/05 Laval para.94.
[139] Supra note 102, paras.80-85.
[140] Ibid. para.85.

Furthermore, this divergence in legislation and jurisprudence entails unavoidably the risk of forum shopping, as it permits the creation of divergent levels of intellectual property rights' protection and data protection within the European Union.

Until relevant specific Community legislation is laid down, although the balancing process is not a panacea for all situations in the war against digital piracy, especially when so tough constitutional questions are at stake, balancing of copyright and other fundamental rights is the most suitable solution, since a society without appropriate legal copyright and data protection suffers losses, as its copyright owners "*lack the incentive to go on being creative and making a living form their work*"[141], whereas "*consumers will only readily take up new digital services if they are reassured that their personal data is sufficiently protected and not abused for marketing purposes or worse*"[142].

[141] Becker, F. (2007), Market Regulation and the "Right to Property" in the European Economic Constitution. *Yearbook of European Law. 26 (1): 255-296.*

[142] Koempel, F. (2005). Data Protection and Intellectual Property. *Computer and Telecommunications Law Review 11(6) pp. 185-187.*

BIBLIOGRAPHY

BOOKS

Akrivopoulou, C. & Psygkas, A. (2010) *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*. IGI Global.

Dixon, P. & Gellman, R. (2011). *Online Privacy: A Reference Handbook*. Santa Barbara, California: ABC-CLIO, LLC.

Klang, M. (2005). *Human rights in the digital age*. London: GlassHouse Press.

Lessig, L. (2004). *Free Culture: How Big Media uses technology and the Law to lock down culture and control creativity.* New York: The Penguin Press.

Lloyd, I. J. (2008). *Information technology law*. New York: Oxford University Press.

Lucchi, N. (2006). *Digital Media & Intellectual Property/ Management of Rights and Consumer Protection in a Comparative Analysis.* Germany: Springer.

Meyer, S. (2013). *Understanding Digital Piracy*. New York: The Rosen Publishing Group, Inc.

Negroponte, N. (1995). *Being Digital*. London: Hodder and Stoughton, Ltd.

Reed, C. & Angel, J. (2007). *Computer law: the law and regulation of information technology*. New York: Oxford University Press.

Schwabach, A. (2007). *Intellectual Property: a Reference Handbook.* Santa Barbara, California: ABC-CLIO, Inc.

Schwartze, J. (2006). *European administrative law.* Revised ed. London: Sweet & Maxwell.

Stiglitz, J. (2002). *Globalization and its Discontents*. New York: W.W. Norton & Company, Inc.

Tridimas, T. (2006). *The General Principles of EU Law*, 2nd ed. New York: Oxford University Press.

ARTICLES

Aguiar, L. & Martens, B. (2013). Digital Music Consumption on the Internet: Evidence from Clickstream Data. *European Commission Joint Research Centre Institute for Prospective Technological Studies Luxembourg: Publications Office of the European Union*.

Alexy, R. (2013). Balancing, constitutional review, and representation. *International Journal of Constitutional Law 11(3).*

Becker, F. (2007), Market Regulation and the "Right to Property" in the European Economic Constitution. *Yearbook of European Law. 26 (1): 255-296.*

Belleflamme, P. & Peitz, M. (2010). Digital Piracy: Theory. *CESIFO Working Paper No. 3222.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1698618.

Boldrin, M. & Levine, D. K. (2009). Against Intellectual Monopoly. Syracuse Science & Technology Law Reporter. Vol. 21, Art. 6.

Castelluccia, C. & Narayana, A. (2012). Privacy considerations of online behavioural tracking. *European Network and Information Security Agency (ENISA).* Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking/at_download/fullReport.

Chevallerau, F. (2005). The impact of e-government on competitiveness, growth, and jobs. *The IDABC eGovernment Observatory of European Communities.* Retrieved, from http://europa.eu.int/idabc/egovo.

Coudert, F. & Werkers, E. (2008). In The Aftermath of the Promusicae Case: How to Strike the Balance? *International Journal of Law and Information Technology © Oxford University Press. Vol. 18, Issue 1 pp. 50-71.*

Geiger, C. (2009). Intellectual property shall be protected!? Article 17(2) of the Charter of Fundamental Rights of the European Union: a Mysterious Provision with an Unclear Scope. *European intellectual property review, 31*(3)

Groussot, X. (2008). Rock the KaZaA*:* Another Clash of Fundamental Rights. *CMLRev*. *45*, p.1760.

Hetherington, L. (2008). Peer-to-peer file-sharing – ISPs and disclosure of user identities. *Entertainment Law Review. 19(4).*

Hickey, A. (2002). Between Two Spheres: Comparing State and Federal Approaches to the Right to Privacy and Prohibitions Against Sodomy. *111 YALE L. J. 993, 994 n. 8.*

Hunton & Williams, Kuner, C., Burton C., Hladjk, J., Proust, O., Manak A., Högberg A. C. (November 2009). *Study on Online Copyright Enforcement and Data Protection in Selected Member States.* DG Internal Market of the European Commission. Retrieved from http://ec.europa.eu/internal_market/iprenforcement/ docs/study-online- enforcement_en.pdf.

Johnson, M. E., McGuire, D., Willey, N. D. (2008). The Evolution of the Peer-to-Peer File-Sharing Industry and the Security Risks for Users. *Proceedings of the 41st Hawaii International Conference on System Sciences*. Retrieved from: http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/publications/pdf/30750383_1.pdf.

Koempel, F. (2005). Data Protection and Intellectual Property. *Computer and Telecommunications Law Review 11(6) pp. 185-187.*

Kisieliute, I. (2012). *A "fair balance" between intellectual property rights and other fundamental rights?* (University essay). Lund University, Sweden.

Lim, D. (2007). Beyond Microsoft: Intellectual Property, Peer Production and the Law's Concern with Market Dominance. *Fordham Intellectual Property, Media And Entertainment. Law Journal.* Vol. 18, Iss. 2.

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145*.

Morris, P. S. (2009). Pirates of the Internet at Intellectual Property's End with Torrents and challenges for choice of law. *International Journal of Law & Information Technology, 17(3), 282-303.*

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, Vol. 57, p. 1701*.

Peukert, C., Claussen, J., Kretschmer, T. (2013). Piracy and Movie Revenues: Evidence from Megaupload: A Tale of the Long Tail? *Social Science Research Network (SSRN)*. Retrieved from http://ssrn.com/abstract=2176246.

Rantou, M. (2012). The growing tension between Copyright and Personal Data Protection on an online environment: The position of the Internet Service Providers according to the European Court of Justice. *European Journal of Law and Technology, Vol. 3, Issue 2*.

Robison, W. (2010). Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act. *Georgetown Law Journal, Vol. 98, No. 4, 2010*.

Rubenfeld, J. (1989). The Right of Privacy. *102 Harv. L. Rev. 737, 749*.

Santucci, G. (2013). Privacy in the Digital Economy: Requiem or Renaissance? *The Privacy Surgeon*. Retrieved from http://www.privacysurgeon.org/blog/resources/gerald-santucci-paper/.

Tene, O. (2011). Privacy: The New Generations. *International Data Privacy Law 1 (1): 15-27, first published online October 5, 2010.*

Warren & Brandeis (1890). The right to privacy. *Harvard Law Review. Vol IV no 5*.

Warrior, J., McHenry, E., & McGee, K. (2003). They Know Where You Are. *IEEE Spectrum, vol. 40 no. 7, pp. 20-25*.

Wong, R. (2004). Privacy: charting its developments and prospects. *Human rights in the digital age. London: The Glasshouse Press*.

Wright, T., Liotta, A., Hodgkinson, D. (2008). E-privacy and copyright in online content distribution: a European overview. *World Data Protection Report. BNA International. Volume 8, Number 5.*

Yali, T. *Copyright and privacy: Their Interaction in the Context of Peer-to-peer Networks*, (Master thesis). Leiden University, Holland.

LEGAL TEXTS

Charter of Fundamental Rights of the European Union, Official Journal of the European Union C 83, 30.3.2010.

European Convention of Human Rights and Fundamental Freedoms. 4 November 1950, 213 U.N.T.S.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108.

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281 , 23/11/1995 P. 0031 – 0050.*

Directive 2000/31/EC (Directive on certain legal aspects of electronic commerce in the Internal Market, commonly known as the "E-Commerce Directive").(Official Journal L 178 of 17.07.2000).

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society. (Official Journal L 167 of 22.6.2001).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Official Journal L 157 of 30.4.2004).

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.

Universal Declaration of Human Rights, Council of Europe (CoE) Convention for the Protection of Individuals.

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and related acts. Official Journal C 340, 10 November 1997.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, Official Journal of the European Union C 306, 17.12.2007, 1-271.

CASE LAW

Judgment of the Court, 13 July 1989, Case 5/88, Wachauf and Bundesamt für Ernährung und Forstwirtschaft, ECR 2609.

Judgment of the Court, 12 June 2003, Case C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich.

Judgment of the Court, 6 November 2003, Case C-101/01, Bodil Lindqvist, Official Journal C 7, 10.01.2004.

Judgment of the Court, 14 October 2004, Case C-36/02, Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn.

Judgment of the Court (Grand Chamber), 18 September 2006, Case C-479/04, Laserdisken ApS v Kulturministeriet.

Judgment of the Court (Grand Chamber), 18 December 2007, Case C-341/05, Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet.

Judgment of the Court (Grand Chamber), 29 January 2008, Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU.

Judgement of the Court (Grand Chamber), 16 December 2008, Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia.

Judgment of the Court (Third Chamber), 5 May 2011, Case C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland.

Judgment of the Court (Grand Chamber), 3 September 2008, joined cases C-402/05 P & C-415/05, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities.

Judgment of the Court (Third Chamber), 24 November 2011, Case C-70/10, Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM) ECtHR Case Balan v Moldova, January 24, 2012.

Godfrey v. Demon Internet Ltd., [1999] 4 All E.R. 342 (Queen's Bench Division, March 26, 1999).

A&M Records, Inc. v. Napster, INC., 239 F.3d 1004 (9th Cir. 2001).