UiO : Faculty of Law
University of Oslo

Towards a new Digital Rights Management ecosystem: The importance of its systems for the copyright holders, the consumers and the innovation. The example of the HTML 5.

Candidate number: 8010

Submission deadline: 01/12/2014

Number of words: 16.140

Table of Contents

INTRODUCTION

Law, technology and society, form a triangle which includes the concept of Digital Rights Management and they are continuously interacting with each other, affecting the economy and innovative spirit, in tandem. The social and economic development are, also, affected by the existing platforms of securing copyright and are directly connected to the mechanisms provided by our information society. The intellectual property phenomena, in particular in United States and Europe, the evolutionary economics approach supported by the analogous internet technology evolution, across the socio- legal theories, lead to an interesting synthesis of aspects regarding the necessity and effectiveness of Digital Rights Management technologies.

The concept of DRM provides the importance of the tools used for the success of its purpose. The market and the rapid growth of e-commerce increased the interest of re-defining the meaning of openness on the internet, the importance and impact of file-sharing and the effects of digitalization. Once Tim Berners-Lee founded the World Wide Web[1] Consortium and applied the Hyper Text Markup Language (HTML), users without much technical know-how were able to perform their creative work online. Lawrence Lessig[2], predicted possible restrictions that the disposal of knowledge could have under the copyright and proposed the successful Creative Commons in favor of society and research.

This work focuses on the DRM as a leading norm- shaping regime[3] in culture, entertainment and the artistic world regarding its direct connection to copyright. The DRM and its mechanisms appeared as the main effective technical protective solution for publishing and the entertainment industry.

---

[1] http://www.w3.org

[2] http://www.lessig.org/about/

[3] Schollin Kristoffer: Digital Rights Management, The new copyright, Jure Forlag AB, Stockholm, 2008, pg.16

The evolutionary character of the Information Society enshrines the attempts to defend intellectual property rights in a way that could cause controversial reactions by those that are part of that Society. An example is that in the latest version of HTML, the HTML 5; a DRM mechanism based on encryption technology imposed in order to prevent illegal file sharing and detecting inappropriate and unlicensed use.

The aim of this work is twofold: firstly, to describe the framework of the legal position of DRM in the world of intellectual property rights and secondly, to describe some of its technologies as an example through which it is possible to discuss the consequences of such applications on innovation and society.

The legal method that has been chosen is descriptive and based on a parallel presentation of the DRM mechanisms, techniques, platforms and necessities that created it with the main impacts to its existence in the internet world. This method has been chosen because the legal framework will be better comprehended if some interdisciplinary and empirical information is provided. The major legal instruments in Europe, providing the implementation of the DRM technology, have a crucial position in this presentation, as well. The purpose of this methodology is to see the historical origins of DRMS and their impact to legal rules.

The research aims to analyze the legal provisions regarding the DRM, to identify the international instruments and evaluate the current policy and legislation in EU and US. These two major geographical areas and their legislation have been chosen because of their impact worldwide. The influence of the online content providers to intellectual property rights is based on industries established in US and EU, where the technological evolution changes the online landscape day by day. The work will include a review of statutes and other legislation, case law, common law, textbooks and articles as well as electronic material obtained from various internet sites.

The hypothesis that expresses my thesis is that the DRM systems currently are in a transitional stage and create an ecosystem that is based on more flexible technical platforms compared with the applications of the past decade, tending to be more personalized regarding the use of content by the lawful user. The legal hypothesis is this: The evolutionary

character of technology leads the *code* to be treated as law when we examine the current phase of DRM and its systems.

Definitions

Digital Rights Management (DRM) refers to protecting digital data from unauthorized copying, distribution, access and data that include asserted rights and need to be managed. It is an access and usage control technology, usually software, based on encryption, used by copyright holders to limit usage of digital content. DRM Systems can be also viewed as instruments to enable digital distribution platforms where innovative business models can be implemented[4]. DRM is being used by content providers (CP) to protect their rights by preventing access to unauthorized users as well as preventing copying or converting digital data into another format even by authorized users[5]. We could categorize the DRM systems to those systems that protect access to content and also limit the copyright and the transferring of content from one device to another. Also, parts of DRM are the technologies outside the scope of a DRM implementation, but are auxiliary to its aim, like the identification systems. One of these, widely used technologies online, is the digital watermarking.

The term *Digital Rights Management* includes the aspect of digitalization, which means that it is used broadly in a tight connection with the occurrences of copyright and the accessibility to those rights in the online world. Hence why, the technologies can be combined in order to monitor, identify and enforce the usage of intellectual assets in any digital format. These assets can be photos, created artistic works, articles, databases, and software programs, to name a few.

The term *Technical Protection Measures* (TPM) can be used interchangeably with DRM. The term TPM denotes a theoretical claim under which a certain system has specific capabilities as a digital rights system, in terms of being worthy of legal protection. The TPM are

---

[4] Bechtold Stefan: From Copyright to Information Law-Implications of Digital Rights Management, in Security and Privacy in Digital Rights Management, Lecture notes in Computer Science, 2002, at http://link.springer.com/chapter/10.1007/3-540-47870-1_14

[5] Asoke K. Talukder, Manish Chaitanya, Architecting Secure Software Systems, CRC Press, 2008, pg.302

related to the authorized use of digital content. An integral part of DRM systems is the *Rights Management Information* (RMI), which intends to identify a work in the digital format, giving information about the creator and the owner of a right related to that work. Like the TPM, the RMI evaluates a technological construct in order to have a legal protection, as well.

As a technological platform, the DRM has the ability to transform the way that the intellectual property rights are perceived by humans to a language readable by software programs based on encryption and relative technical languages. Such technology uses metadata in order to reach its aims and it is known as *Rights Expression Language* (REL). For the purpose of this work a short explanation of these two terms is useful in order to have an overall of the functionality of DRM in the legal EU and US construction.

The use of metadata by the search engines determines what the content of a web page is and the relevance of the content to a given search. This type of data is included to the, so-called, *meta tags* in a web page`s HTML or XHTML. The usual type of metadata includes the type of the content found on a web page and its description, the title of the content which is shown in the results of a web page and additional keywords provided by the search engine and related to the content present on that page.

The Rights Expression Languages (RELs) are languages devised to express conditions of use of digital content. They have been proposed to describe licenses governing digital content[6]. The REL support, in a reliable and consistent way, the interoperability among various different systems and platforms, in the online environment. Its main function is to define licenses and permission with regard to document content usage. REL facilitates the association of digital rights to digital content. The majority of RELs are, usually, inserted as metadata in documents like MP3 audio, e-books or downloaded video. A common online REL is the General Free Documentation License (GDFL), which gives users the permission

---

[6] Serrão Carlos , Jaime Delgado, Miguel Dias, i-DRM- interoperable Digital Rights Management, VDM Verlag Dr. Muller, 2009, paragraph 2, page 77.

to copy and distribute a work for free. The Moving Picture Experts Group (MPEG-21) and the Open Digital Rights Language (ODRL) are some significant examples of RELs.

The five chapters will be analyzed as follows: The first chapter refers to the nature and history of DRM, the techniques and applications, the typology of DRMS and the effectiveness of its performance. In the second chapter the legal framework regarding the implementation of DRM systems in the examined judicial regime of European Union will be presented. The third chapter will focus on the judicial treatment of DRM in Europe and the position of DRM in the US legislation. The concept of *fair use* as crucial in copyright online and the *piracy* in order to justify the implementation of DRMS by content providers will, also, be discussed. In the fourth chapter the issue of interoperability in the DRM world and the concerns regarding the consumer protection will be analyzed. Lastly, in the fifth chapter, we will attempt to examine the impact that DRM mechanisms have to innovation and the spread of knowledge in order to become approachable. The part of HTML 5 in the world of DRM will be discussed, as well.

1 CHAPTER 1 . The nature of Digital Rights Management

1.1 Functions and Typology of DRM

The digital content provider based on DRM systems can control the quantity and quality of the copies that can be made by a user. The limits that can be set up vary from the absence of permission allowed, up to unlimited permission of copying. So, for example, when appeared in the market, we could see in the iTunes platform, only a set of song copies allowed by the EMI`s Copy Control DRMS. The character of the copies was not permanent, having a deadline of online presence. The data area of the disc included DRM copies with a restriction of the audio content in order to prevent the removal of the content from one medium to another.

In the internet world a form of prevention is the ability of a *stream* to be captured while it transmits the packets of information.

The term *circumvention* of a system is used on a digital level, when a DRM System becomes ineffective to fulfill its requirements after the intervention of an external factor or a third party. In DRM systems there are several strains regarding the degree of facilitations related to preserving or boosting innovative business models. The business model of a DRM system tries to maintain the current establishment on the market and in this form is considered as unfriendly to innovation.

Facilitation and constraints are factors that can be altered in the world of digital rights. The retention of the online content could give the copyright holder the ability to change either the content of the stored information or the terms of accessibility to this particular content. The content can possibly be keyed in order to be reachable only by certified devices and /or software. The right-holder, in this case, could control the content online remotely, having the advantage of altering the content or retaining the control of its use. This particular DRM system needs continuous updating in order not to be circumvented by hacking practices.

1.2 The components of a DRMS. An example

The Open Intellectual Property Management and Protection (OpenIPMP[7]) is a DRM system, supporting the management and securing digital assets. It is the base of applications included in platforms used by Nokia. Even if it is not a wide spread platform, it is useful as an example, because it has all the necessary components of a DRM and it has been tested successfully in the market. It encompasses a number of standards for audio and video, intellectual property management and protection programming as a multimedia file format. The system combines a type of identification of the user and content, user management, encrypted content based on algorithms and the protection of the distribution channel. It,

[7] http://sourceforge.net/projects/openipmp

also, uses open standards like the DRM signaling and MPEG-4 specifications. These are the key elements of the OpenIPMP. Considering the identification of every user in the digital environment, the system follows the procedures of digital certificates, issued by a certificate authority, in order for the identity of the end-user to be ensured. Regarding the user's identification, the system uses Digital Objects Identifiers (DOI)[8], designed to update, in a dynamic way, the metadata referred to a specific digital asset.

Also, an essential part of the OpenIPMP is the License Management, supported by a technical form, which allows definitions of permissions and agreements with the rights holders and the cryptography, as a means for encoded and encrypted information. However, without going deeper into technical details, a DRM system intends to provide security, both to the right-holder and to the customer. It is interesting to mention that apart from the existence of the Open DRM systems, the market presents some Close DRM systems, where the constraints for the consumers seem to be strengthened. Two of them were the applications by the Windows Media Player and Apple`s *Fairplay* imposed in iTunes. These two systems were not interoperable, so the user was unable to use content downloaded from one of the applications, to the other.

1.3 The implementation of DRM in the intellectual property world

The DRM systems are part of the nature of the copyright in the digital era. The expansion of the internet to a broaden consumer base made the goods of entertainment and information reachable by numerous end-users. The music industry was the first business sector affected by the wide spread of its copyrighted work on the internet. In fact, the digitalization of these works transformed the industry to rights management organizations. In the last quarter of the 20th century the increasing of personal computer devices facilitated the file sharing and the *peer to peer* (P2P) technology infrastructure. The latter involves the direct

[8] http://www.doi.org

internet-based communication between two or more agents in order to bypass the computer server.

The development of techniques enabling the ease of storage and transmission of information in a digital environment is springing from the development of digital compression as means for the entertainment industry to facilitate distribution and production of services.

The companies which control the music industry like Sony Music and Warner Music attempted to prevent copying of music by making unplayable audio CDs on computer CD-ROM drives. This was one of the first DRM mechanisms, which included an error that could confuse those CD-ROM drives. The development of standards for video conferencing in 1989 was accomplished by the Moving Picture Expert Group (MPEG). It achieved to reduce the bit rate for moving pictures to an audio CD, with a significant impact to cost and the quality of image. The Video- CD was replaced by the DVD. The development and standardization of the MP3[9] followed the evolution of the high compression standards and it became the basic format for storing and transmitting digital music files. Its popularity continued to rise because of its capability to store files even if the speed of the network was low. The MP4 conforms to computer graphics for a better image quality and is used in iPods. The development of the Internet, the web browsers and the World Wide Web took place together with the digital recording, compression and transmission, allowing internet users to send files to each other in the case of obtaining digitally recorded music.

Napster was the revolutionary platform which made sharing in the digital world more than feasible. It was a search engine, which allowed its users to view and download the contents of MP3 indexes from the hard drives of other Napster users.

[9] http://www.mp3.history.com/en

1.4 Piracy[10], digital theft, file-sharing: The DRM as a necessity

The digital piracy was the necessity that motivated lawmakers to deal with the implementation of TPM in copyright world. The music industry is a classic example of how easy the unauthorized use of copyrighted material has become in the digital environment. According to the Recording Industry Association of America (RIAA) which is the trading organization that supports the creative vitality of the major music companies and protects the intellectual property rights of artists and music labels, digital music theft has been a major factor behind the decline in sales over the past 15 years[11]. At the same time, the RIAA recognizes that during recent years, other forms of digital theft have emerged such as unauthorized digital storage lockers used for the distribution of copyrighted music, stream ripping programs and mobile applications that enable digital content theft. In the United States music sales have dropped by 53 percent since peer-to-peer file-sharing site Napster appeared in 1999.

The most important technical advance was the arrival of BitTorrent. The Bit Torrent file requires the client to make a series of many small data requests, similar to internet telephony which breaks voices into small packets of data. Users, in order to start the downloading, obtain a torrent which is a small file that contains metadata about the file to be downloaded and information about the tracker, the computer that coordinates the file distribution. Pirate Bay is one of the best known torrent website that employs this technology.

Nevertheless, file –sharing technology weakened copyright protection, first of music and software and increasingly of movies, games and books.[12]

The problem that is the unauthorized use and distribution of copyrighted content has expanded to the software industry, as well. The challenge for DRM systems was and, still, is to protect the software, making it compatible with the plethora of devices in a competitive market.

---

[10] Directive 2001/29/EC, Recital 15

[11] http://www.riaa.com/physicalpiracy.php?content_selector=piracy-online-scope-of-the-problem

[12] Felix Oberholzer-Gee and Koleman Strumpf, File-Sharing and Copyright, in http://musicbusinessresearch.files.wordpress.com/2010/06/paper-felix-oberholzer-gee.pdf

1.5 The challenge of Cloud Computing

Cloud Computing and DRM have something in common: they have to convince both the market and the public, about their effectiveness regarding the issues of confidentiality and data security. Cloud computing activities are often described[13] as falling into one or more of the following three service categories:

- Infrastructure as a service (IaaS): raw computing resources, such as processing power and storage
- Platform as a service (PaaS): platforms for developing and deploying software applications
- Software as a service (SaaS):end-user applications

Cloud users may typically run via web browsers and application software installed on remote servers which sends results to users over the internet. This means that relatively simple devices, such as mobile phones or tablets, may be used to obtain access to vast computational resources. Usually, the technical and storage resources are abstracted in cloud computing, and the data control by third parties carries risks. Concerns are often raised about decreased user control and increased provider control over data within the cloud, particularly the security of this data. Confidentiality and integrity are shared in common with DRMS in a cloud computing service. Cryptography, as a DRMS function is essential in data storage in the cloud, as well, but it is not an effective tool when managing data. Unauthorized access is possible if data is intercepted during transmission. If users transmit unencrypted personal data, even via secure channels, providers will still receive unencrypted data as such[14]. The DRMS within the cloud has to follow the protected material in a plethora of applications and devices in order to be effective. This ability demands sophisticated DRMS based on personalization of the service offered. This is, actually, a reason for

[13] Millard Christopher, Cloud Computing Law, Oxford University Press, 2013, pg.3-4

[14] Ibid, pg.22

transposition of DRMS to an advanced level, where can cater to the needs of end-users and the business world.

2 CHAPTER 2 . The DRM in a legal framework

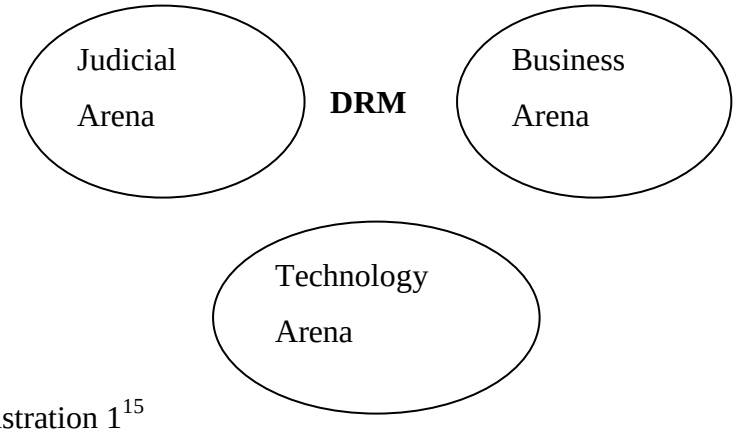

Illustration 1[15]

The DRM can be viewed under two significant aspects:

1. Firstly, as a legal system which takes place in a technological and electronic environment.
2. Secondly, as a system that needs protection under the laws that do not allow circumvention of the DRM mechanisms.

A description of DRM in the legal norms of European Union and how these systems have been viewed by the EU legal construction will take place.

2.1 The copyright in the digital world

The European Community saw in copyright an opportunity to harmonize the internal market[16] affecting the national laws of its Member States in the areas of databases, computer

[15] Schollin Kristoffer: Digital Rights Management, Jure Förlag AB, Stockholm, 2008, pg.328

programs and the internet. The scope of the legislation was to eliminate the barriers regarding the free movement of goods and services. It still is, according to the European Commission, noting the importance of the economic impact of copyright and the indication of the copyright related industries as fundamental in post-industrial society, especially where connected to the information society[17]. The EU, responsible for conducting the negotiations on intellectual property within World Intellectual Property Organization (WIPO), has a view of ensuring protection of Intellectual Property Rights (IPRs) internationally.

More than one copyrights, may have, for example, a book protected as a literate work and another copyright, arisen by the style of its typographical arrangement. A database can have a copyright under the way that its data is arranged and another one because of the content that it may have. Also, a sound track in a film can have a copyright as part of the film or as a sound recording.

The importance of DRM systems is obvious when such systems are imposed by copyright holders in order to prevent the infringement of their work. The digital copyrighted material and the rapid growth of technology led the lawmakers worldwide to act in order to protect the content on the online environment considering potential threats.

2.1.1 The DRM in the World Intellectual Property Organization – WIPO

The WIPO Copyright Treaty (WCT) entered into force on March 6, 2002 and the WIPO Performances and Phonograms Treaty (WPPT) entered into force on May 20, 2002.Both provided the importance of legal protection of TPMs. The importance of the WIPO legal instruments is fundamental because the concept and terminology of the organization was

---

16 Article 115 , Treaty of the Functioning of the European Union (TFEU)

17 http://ec.europa.eu/internal_market/copyright/index_en.htm

the base for the implementation of the DRM systems in the US and EU legislation. The international obligations under the aegis of WIPO were crucial for the expansion and justification of DRM systems in various legal regimes worldwide.

In the preamble of the WCT we read that the contracting parties "*recognize the need to introduce new rules, providing adequate solutions to the questions raised by new economic, social, cultural and technological developments".*

The introduction to an international legal tool of a new form of protection of the work of authors and related right holders, provided the ability of an independent, based on technology protection, for their work,.

Apart from the clarification of the application of the right of reproduction

Article 11 of WIPO Copyright Treaty (WCT) notes that "*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."*

Also, Article 18 of the WPPT, notes that "*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law."*

The key words in both the WIPO and WPPT (articles 11 and 18 respectively), are the *legal protection* with *effective legal remedies* against the circumvention of technological measures used by the right holders in order to protect their rights. The reference of circumvention of the technological measures, used by the creators of copyrighted material in the electronic environment, was the threshold of the introduction of the DRM in the legal construction of WIPO.

Also, WCT Article 12 notes that: (1) "*Contracting parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts*

knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

i) To remove or alter any electronic rights management information without authority;

ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority

Adequacy and effectiveness of the legal remedies are obligations for the Member States that have sprung from Article 12 of WCT regarding the protection of copyrighted work by DRM systems. The Rights Management Information (RMI) definition of Article 12 (2) WCT includes the identification of the online protected work and its author, the owner of the right in the work and/or information about the terms and conditions of use of the work. It, also, includes the encryption that may represent that information and any connection to a copy of the work presented to the public. The unauthorized user of online copyrighted content is in the center of the provisions of Article 12 WCT along with the importance of the relative content of the technical protective measures and its legal protection.

As a global *de facto* legal system executed in a technological construction, when we focus on a specific regional area, the DRM is a phenomenon characterized by legal differences. The European Community and the United States are two of the major players in the arena of technical research and development of measures protecting the copyright using technological measures provided by the DRM. Information, publishing and entertainment industries were in a position to have a considerable impact on lawmakers. Especially, the job market related to creativity and copyrighted content in these two regions depends on how effective a relative protection can be when intellectual property goods launch. The market of China and India, also, is a promising area for the expansion of online copyrighted material. At the same time are the places that the increase of unlawful users of such content demand for DRMS adapted to their market characteristics. The importance of the WIPO legal

instruments is obvious in this case, because the implementation of the DRM concept is easier to achieved as an international obligation.

2.2 The DRM in the legislation of the European Union.

The EU adopted the DRM concept in its 2001/29/EC Directive of 22 May 2001[18] in its Articles 6 under the title *Obligations as to technological measures* and in Article 7 under the title *Obligations concerning rights-management information.*

The main objective of this adoption was to transpose the obligations springing from the WIPO Internet Treaties to the European Community`s legal structure. In the past, the European Commission had expressed its concerns about the development of technical devices regarding their use to control unauthorized copying [19] mentioning the necessary *attention given to the development of technical devices that might be used to prevent or control copying of recorded material.*

It is notable that in the European Community law, already, exist two different legal regimes applicable to DRMs:

1. One was established by the Conditional Access Directive, which applies to television and radio broadcasting by any means, including provisions for "information society services"[20]. According to this regime, it is required by the Member States to prohibit the manufacturing, sale and rental of devices or software that give access to a protect-

---

[18] 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.

[19] European Commission, Green Paper on Copyright and the Challenge of Technology, Brussels, 31 January 1989, 3.6.4, page 119

[20] Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, Article 2

ed service in a digital form if the service provider has not given his/her consent. But, the acts of circumvention or the personal use of an illicit device are not prohibited by this Directive.

2. The other, is the aforementioned Copyright Directive, which prohibits the circumvention of the DRMs and the operation in illicit devices along with the circumventions of services.

The Copyright Directive imposes some obligations to the Member States in order to harmonize their laws on copyright and related rights, by setting specific objectives regarding the establishment of an internal market avoiding the distortion of competition[21].

Another issue the Copyright Directive is concerned with, is the increasing of the legal certainty while providing a high level of protection of intellectual property as a factor of fostering substantial investment in creativity and innovation. The scope is to grow and increase the competitiveness in the European industry. The information technology and the goods of intellectual property, as an integral part of property, are crucial to the EU economy in general[22].The ultimate aim of the technical measures is to protect works from unauthorized use and to provide information regarding the rights connected to the content, giving effect to the principles laid down in law[23].

According to the provision of Article 12 (1), the European Commission expressed an interesting opinion on DRM technologies and the application of the Directive 2001/29/EC,

---

21 Directive 2001/29/EC, Recital 1

22 Ibid, Recital 4 and 9

23 Ibid, Recital 13

which was stated by a relevant report, the first after the implementation of the Directive, acknowledging the importance of these systems regarding the management of copyright[24].

Particularly, Commission reports that:

"In the context of the discussions on the management of copyright and related rights in the new digital environment, digital rights management (DRM) has become a key issue. DRM systems can be used to clear rights, to secure payment, to trace behavior and to enforce rights. DRM systems are, therefore, crucial for the development of new high volume, low transactional value business models, which include the pricing of access, usage, and the service itself, subscription models and reliance on advertising revenue, credit sales or billing schemes. DRM systems are a means to an end, and as such, clearly are an important, if not the most important, tool for rights management in the Internal Market of the new digital services […]. Articles 6 and 7 and relevant recitals deal with the protection of technological measures and rights management information respectively[25]."

Also, " *DRMs do not present a policy solution for ensuring the appropriate balance between the interests involved, be they the interests of the authors and other right holders or those of legitimate users, consumers and other third parties involved (libraries, service providers, content creators...) as DRM systems are not in themselves an alternative to copyright policy in setting the parameters either in respect of copyright protection or the exceptions and limitations that are traditionally applied by the legislature."*

The Commission realized that the implementation of a DRM system cannot replace the legal norms provided for the copyright protection. Moreover, the Commission didn`t intend to provide any alternative policy regarding the copyright management outside the legal infrastructure of Member States and their obligations in EU. The appropriate balance be-

---

24 Communication from the Commission to the Council, the European Parliament and the European Economic and Social - Committee The Management of Copyright and Related Rights in the Internal Market, COM/2004/0261 final

25 Ibid, Paragraph 1.2.5

tween copyright holders and legitimate users has to be the aim of the implementation of a DRM system by any stakeholder.

The Commission found that there was a potential danger related to DRM mechanisms: the parallel creation of a technological regime, which could operate independently of the established legal regimes and threatening the free access to digital information and especially to the information located in the public domain. The accessible information has to be part of the legal construction of the interested states involved and these states are the only responsible for the enforcement of the relevant rights. The Commission has the aspect that the DRM systems can only be an auxiliary means to the state authority when attempts to protect digital works, considering any exceptions.

The Commission's aspect reflects a concern expressed by Lawrence Lessing for the dominion of the *code*[26] in the digital environment and the possibility of no interference of the human factor with subject matter the rights exercising.

A closer analysis to Articles 6 and 7 of the Copyright Directive (also noted as Infosoc in literature) might be enlightening for the position of DRM in EU legislation.

Firstly, in Article 6 (3) of the Directive the DRM concept is defined as "*effective technological measure"* and requires the effectiveness of the system in case of a controlled protected work. The DRM system does not protect the digital work as a single technology but has to operate in a specific architecture of a system. That means that the modules of the DRM can claim the protection of Article 6 (3) only if they contain measures that control access to digital material. The inclusion is related to encryption mechanisms, security of transferred information, user identification and management systems along with constraints of usage of the protected content.

---

[26] Lawrence Lessig, Code V2, online, under the Creative Commons Attribution, page 4, paragraph 4: ¨the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing architecture that will perfect control and make highly efficient regulation possible. The struggle in that world will not be governments. It will be to assure that essential liberties are preserved in this environment of perfect control``.

Secondly, Article 7 (2) of the Copyright Directive provides the DRM under the concept of "*rights- management information"* (RMI). In this case, the right holders provide the relative information for the identification of their protectable work. That kind of information has two characteristics:

The one of those is to offer the means for identification of the work in subject matter or identification of a subject-matter referred to in the Directive or referred to the *sui generis* right for the protection of databases under the Directive 96/9/EC.

The other, is related to the information provided by the right holder regarding the terms and conditions of use of the work in the digital environment and numbers or codes, if present, representing that information.

In the case of Article 7(2) the law provides the recognition of the rights based on technological means that are able to distinguish between the nature and the degree of the permission in a work.

2.3 Circumvention and Copyright infringement

The right established by the Copyright Directive does not constitute a new intellectual property right but an auxiliary right to the exclusive rights of the author.

- *"Effective technological protection measure"*

The protection under Article 6 of the Copyright Directive is given to those DRM systems which comply with the criterion of *effectiveness*. The definition and specification of the means of a measure in order to be effective is lacking even if it is mentioned in both article 6(1) and (2). The attempt to be given one meaningful definition is not so successful. This definition (in article 6) is not a model of clarity[27].

---

[27] Study on the implementation and effect in Member States` Laws of Directive 2001/29/EC, Final report, Institute for Information Law, University of Amsterdam, The Nederlands, February 2007, 3.2.1, page 75, paragraph 2

The legislator intended to grant protection to devices whose circumvention would not be easy or possible under an ordinary attempt. The DRMS in that case

1. Has a degree of control over the use of the protected work and achieves the objective set by the law in order to be effective and
2. Fulfills the requirement of effectiveness under the principle of proportionality, which has to be demonstrated for the objective of protection to be achieved[28].

- *"Designed to prevent or restrict acts not authorized by the right holder"*

A legal uncertainty arising from this quote could affect the way that a Member State applies the law. For example, the scope of DRM systems in Article 6 (3) can be interpreted as capable to be protected in case of being designed solely for the purpose of controlling works under copyright. It has not, also, been clarified whether there are any essential requirements or there is such an essential requirement connected directly to the prevention of copyright infringement and the use of a DRM mechanism. The European Court of Justice, in Nintendo Case, noted that it is necessary to be examined the purpose of device provided for the circumvention of protection measures, taking account of the use which third parties actually make of them, according to the circumstances at issue. The effectiveness need not be absolute[29]. The national court may examine how often DRMS are used in disregard of copyright and how often they are used for purposes which do not infringe copyright.

A relevant topic related to the effectiveness of a DRM system establishes Article 6 (3) of Copyright Directive when the system is programmed to control the copy and the access to a protected content. The *access* and the *protection* of copyright are two different objectives under the Berne Convention. The issue of access to a copyrighted work should explicitly be declared in the Directive. The involvement of DRM technology as means to access protected works could embed the lack of protection under the Directive. But, digital works in-

---

[28] Recital 48, Copyright Directive

[29] Case C-355/12, ECJ, Judgment of the Court of 23 January 2014 (request for a preliminary ruling from the Tribunale di Milano, Italy), Nintendo Co. Ltd and others Vs PC Box Srl, 9Net Srl

volve, by nature, the –at least temporary- making of a copy in a user`s device. So, it is necessary copy and access to be protected against circumvention attempts by the Member States. Under this realistic scenario the use of DRMs allows the right holder a *de facto* right of access to the digital content. The concept of adequate legal protection is part of the WCT in its Article 11.

- *The "adequate legal protection" of Article 6 (1)*

In Article 6 (1) of the Copyright Directive the meaning of the affordable protection in order for it to be *adequate*, is not clear. Combined with Article 6 (3) we can see that whether or not the DRM right is granted to authors regarding their rights has not been defined. It is, also, not clear what is the kind of the protection the right holder is entitled to exercise. For example, if his/her rights are financial or moral.

Article 6 (1) does not identify who has to ask for the protection. In practice, both the right owner and the authorized intermediary can have a right to protection, as an agent or licensee. Also, the same article lacks specification as to whether the technological measures in use have to be connected with the exercise of a right or the same measure has to constrain acts not permitted by the law and they have not the approval by the right holder. Hence, there is not a direct connection between the copyright infringement and the circumvention of technology measures that protect copyrighted material. The Member state, has to specify the grade and the nature of the legal protection that offers to right holders under the Article 6 (1) and (3) without a clear guidance by the Directive itself.

- The "*adequate legal protection"* in Article 6 (2)

The use of products or services that enable, facilitate or prepare the circumvention of DRMs is prohibited under the provisions of Article 6 (2).

The affordable legal protection is declared in Recital 48 of the Copyright Directive, where "*legal protection should be provided in respect of technological measures that effectively restrict acts not authorized by the right holders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development.*

Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography."

The adequate legal protection is related to actions of manufacturing, importing, distributing, renting, selling, advertising, possessing for commercial use devices, products, components or providing services which "*(a) are promoted, advertised or marketed for the purpose of circumvention of, or (b) have only a limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures*[30]*."*

Article 6 (2) does not allow any commercial trade which involves devices that facilitate the circumvention of DRMs as well as services and advertisements (including the online ones) that promote such illegal use of applications. The circumvention devices that provide protection against copyright infringement and the ones that do not provide it, are not distinguished in Article 6 (2), making the connection between copyright protection and the legal protection against a specific trade of devices, vague . A probable legal tool, useful for the distinction, could be the aforementioned criterion and principle of effectiveness and proportionality relatively.

---

[30] Article 6 (2) EUCD

In my opinion, the provision of Article 6 (2) b) should have provided clearer guidelines regarding whether or not a device or application should be able to have a *limited commercially significant purpose or use other than to circumvent* .For example, how can the commercial significance of an action related to a circumvention be estimated or on what base could the qualitative limitations imposed by the Member State`s authorities be set for the purpose of circumvention to be clarified? The accountability of the evaluation of these factors is part of the case-by-case examination by the courts. The contribution of ECJ regarding this point is noticeable in the aforementioned Nintendo Case.

The Court`s answer notes that:

1. The TPMs can be rightfully implemented as an attachment to copyright-protected works. This does not only include the implementation in the physical support (e.g. Blue –Ray) but in the hardware device as well, which is capable of reading the content. The TPM, for example, can be implemented in the gaming console.
2. The legal protection of copyright holders will not be an obstacle for activities, whose principle purpose is not to circumvent and to avoid the technological protection of games.
3. The legal protection must respect the principal of proportionality in any case and includes the devices, too.

When it comes to deciding whether the TPM are legally imposed or not the key aspect is the *actual use*, made by third parties. This actual use regarding the devices, products or components which have the functionality of enabling or performing the circumvention includes, also, purposes which do not infringe copyright. Such purpose could be the playing of alternative formats of audio or video (e.g. mp3). In this regard, the legality of these measures will be determined by its utility from point of view of the one who is using them. The challenge for the national court will be to determine and get documentary evidence of this actual use. The same court will define the effectiveness of the technological measure provided by Article 6(3) EUCD.

3 CHAPTER 3 . Judicial treatment of DRMS in Europe and US

Regarding the private coping exception and the DRMs a French court decision known as the *Mulholland Drive* case from the Cour de Cassation[31] dealt with the issue. Mr M. Perquin, supported by the consumer organization Union Federale des Consommateurs- Que Choisir, filed suit against the movie studios because he was unable to make a copy of a DVD he had bought, of the American movie Mulholland Drive. The inability was caused by the DRM mechanism related to the copy protection included in the commercial DVD release. The Cour de Cassation interpreted the law in the light of the provisions of EUCD and the Article 9 paragraph 2 of the Berne Convention. In particular, this paragraph introduces the *three-step test* in the copyright law providing that"…*such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author"* .The Court held that the private use exemption could not be as a valid reason to be allowed to bypass DRM. The normal exploitation of the work should be appreciated by taking into account any economic effect that could have such a copy regarding the digital environment. Because of the possible risks that private copying could include in this digital environment the private copying exemption must produce a return to the investment has been by the DVD editors, which in this case didn`t defined under the EUCD.

The French Supreme Court noted that the private copy exception was not an absolute right, but an exception to author`s right and had to be interpreted strictly. The private copy exemption didn`t apply because the risks of infringement online hadn`t been taken into account and hadn't any relation with the normal exploitation of the work. In this case the court found that the interests of intellectual property right-holders prevail against the private copy exception regarding the DRMS.

---

[31] Court of Cassation (1st chamber, civil section), 28 February 2006, Studio Canal, Universal Pictures Video France and SEV v. S. Perquin and UFC Que Choisir , as cited in http://merlin.obs.coe.int/iris/2006/4/article20.en.html

Both, the Copyright Directive and Section 1201 of the US Copyright Act consider the acts of circumvention as *per se* unlawful. Hence, each act of circumvention inevitably draws liability, regardless whether of the type of the use is lawful or not.

3.1 The *ex-ante* exemptions and the *ex*- post evaluations

The functionality of the Technological Protection Measures is based on the *ex ante* programming of access to the protected work online. A problem that arises is related to the free uses of this digital content and the access to it without the consent of the copyright owner. In the Copyright Directive the copyright exemptions are provided by the Article 5, which attempts to compromise the *droit d` auteur* systems, where the exceptions are set *ex ante* , and the US *fair use* doctrine as well as the *fair dealing* of UK , where the fairness of uses are determined by the court, *ex post.* The specific uses that the Copyright Directive provides as exemptions, do not comply with a system that includes these exemptions in a pre- programmed technology under an *ex ante* defined logic. Any restrictions have to be in the DRMs in a time before its circulation in use. They, also, have to be translated into a Rights Expression Language (REL). The wording of Article 5 of EUCD, in practice, cannot provide a solution that could combine a formulation of open-ended principles in order to eliminate legal uncertainty. The opportunities of *ex post* judicial review of the, imposed restrictions by the DRM, to fair use, are reduced because of the limitless anti-circumvention protection offered by the Articles 6 and 7 of EUCD across with the *ex post* enforcement of the three-step-test.

Sometimes, the lawful character of a circumvention of a means by a user could be recognized under Article 5 of the Copyright Directive while the Article 6 (1) of the same Directive could not exempt its liability for the action of circumvention. The provision in this part considers the circumvention as a completely independent illegal act. Being *per se* illegitimate, any act of circumvention is liable irrespective the character of the use, lawful or not, because the anti- circumvention law is not related to copyright infringement. Only certain modules of uses can be protected from access restrictions, defined *ex ante* in the DRMS world. In the US Copyright Act , Section 1201 the exemptions are related to acts by

non- for-profit libraries, educational institutions, archives and purposes of law enforcement, encryption research, to mention but a few.

The EUCD provided the circumvention prohibitions as having a potential unlimited character. The unauthorized access is *de facto* excluded. This probably it is based on the nature of the Directive, which provides as the ultimate evaluator the Member State`s national legislation, where has to be addressed any claim by the user. This character of the EUCD leads the copyright holder, controlling the access to digital works , to exchange the authorization to access with the user`s assurance that he/she will not start actions related with the legal protection of TPM. The DRM technology has the ability to exclude unauthorized access to protected material online, so it is unclear the provision for the user to have a previous permission of the copyright holder, in order to use the material under the conditions of Article 6(4) EUCD.

The DRM technology has the ability to be flexible in setting permissions and constraints regarding the usage conditions of digital copyrighted material. On the other hand, it is weak to provide the numerous possible uses that the copyright uses can include. The DRM systems have, by their nature, the characteristic of restricting the *ex post* evaluation of end-user behavior. The technology the DRM systems is based on and the RELs can include only pre-defined forms of usage of the protected material.

The most complex transformative uses, as the purposes imposed by the research or education, call for more sophisticated DRM systems. Regarding this, the lawmakers have to pay attention to fair uses and the options that enforcement policies can be provided by the *lex informatica*[32].

[32] Joel Reidenberg , Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Volume 76, number 3 , February 1998 at http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship

3.2 The DRM in the United States legislation

The United States Digital Millennium Copyright Act (US DMCA) was enacted in 1998, implementing the WCT and the WPPT. A new chapter, the 12th, is added to Title 17 of the U.S. Code, in particular the section 1201.

The DMCA by creating the legal platform for launching the global digital on-line marketplace for copyrighted works, aimed to make available, via the internet, the movies, music, software and literary works that are the fruit of American creative genius[33]. Section 1201 defines three different types of anti- circumvention violations, which are as follows:

1. The basic provision in paragraph (1) (A) of 1201. According to this, "*no person shall circumvent a technological measure that effectively controls access to a work protected under this title*." For example, it is illegal for a user to hack the requirement of a unique serial number that is necessary during the installation of a computer program.

2. The prohibition on trafficking, which is included in paragraph (2) provides that "*no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:*

A) Is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

---

[33] As cited in David`s Nimmer, A Riff on Fair Use in the Digital Millennium Copyright Act, January 2000, University of Pennsylvania Law Review, VOL. 148, page 681.

(C) is marketed by that person or acting in concert with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title."

This ban prohibits computer repair services from assisting a librarian in the preservation of software stored on decaying media and it prohibits librarians from developing a technology to facilitate circumvention[34].

3. The additional violations in 1201 (b) include almost the same phrasing and prohibit trafficking in devices, applications or services, in order to enable the circumvention of a DRMs if that protects a copyrighted content.

The effectiveness of the technological measures that control access to a protected work is the subject matter of the protection that is offered by the DMCA. These technological measures are divided into two categories: the first includes the access- control measures and the second one is related to copy-control measures.

3.3 The judicial treatment of DRMS in the US

The problem of online infringement, even though the restraints by the DRMs are high, is still a current issue. Bruce Lehman, the responsible person for the anti- circumvention provisions of DMCA, admitted that the strategy to prevent the copyright infringement online, based on DRMs, has failed[35]. In practice, circumvention devices and infringing copies are available online. The online infringement requires a dedicated user to have circumvention software. The availability and popularity of infringing files from DRM- restricted media continues.

A case that could show how the DRMs legislation was treated by the courts is that of The Chamberlain Group, Inc. vs Skylink Technologies, Inc.[36] The case was related to anti-

---

[34] Bill D. Herman, The fight over Digital Rights, Cambridge University Press, 2013, page 44 , paragraph 2

[35] Ibid, p.165

[36] Case: The Chamberlain Group, Inc. Vs Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004)

trafficking provision of the DMCA, 1201 (a) (2). The companies were activated in the garage door opener business sector and the Skylink created a remote opener, capable to interoperate with existing relative systems. The opener, also, could bypass the code system of Chamberlain. The court found that the goals of the DMCA were to establish a balance between the competing interests of content owners and information users and balance access control measures with fair use.

Chamberlain had to prove that they had ownership of a copyrighted work which it was controlled by a technological measure that was circumvented. Also, had to prove that this technological measure could be accessible by third parties without authorization in a way that infringes rights protected by the Copyright Act. The product that is the tool for the infringement had to be designed or produced for circumvention as well as marketed in order to circumvent the controlling technological measure. The Court found in its decision that the Chamberlain failed to show the link between access and protection. Also, it was not explained how the access provided by Skylink`s device, enables the infringement of any right that protects the Copyright Act. Since the activity lay outside the copyright law, the act of bypassing the encryption was not a case of circumvention in the legal sense.

The Court, also, found that the goals of the DMCA were to establish a balance between the interests of content right holders on one hand and users of information on the other, balancing the access control measures with the doctrine of fair use. The fair use in this case, might apply to a circumvention device that is limited to be used.

From case to case the result is the same, while access controls occur before use control and courts seem to find a violation under the 1201 (b) DMCA without finding an access violation. But in any case the use is not feasible without access.

Like in the case RealNetworks vs. Streambox[37], where the software of RealPlayer allowed users to play media files available online. In order to ensure that media files distributed using the proper RealServer software by the RealPlayer clients, the RealNetworks used an authentication application. Streambox, as a subcontractor of Sony, created a software pro-

[37] RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

gram circumventing the authentication application of RealNetworks, allowing users of Streambox to receive files of RealServer. Judge Pechman found violations of 1201 (a) and 1201(b) DMCA.

3.4 The DRMS, the fair use and the three- step- test

The courts in US have to implement the fair use doctrine regarding the copyright infringement on a case by case basis, in order to identify if the infringer is liable on not for infringement. Digital content owners have the ability to decide who makes copies and the conditions of copying. In the world of this digital content, practices that used to be considered as `fair` in the analog copyright world, have no place. The doctrine of *fair use* is included in the DMCA 1201 (c) (1) where "*nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use*…"

"The market for digitally locked goods will no longer need a fair use doctrine, because the market failures and high transaction costs associated with non- protected content will disappear[38]". The comment probably represents an optimistic scenario.

The Copyright Directive in its Article 5 applies exceptions that are allowed to circumvent DRM mechanisms in order to be protected the fair use of copyrighted materials. The difference between this legal tool and the DMCA is noticed in these following points:

- The distinction between *access controls* and *use controls* in EU Copyright Directive is absent
- In Article 6 (4) subparagraph (4) of the Copyright Directive are listed some exceptions that apply only to circumvention acts as these are defined in Article 6 (4) (1), excluding the trafficking in circumvention technology. The prohibition against to trafficking regarding possible exceptions to technology used to circumvention is a

[38] Ben Fernandez, Digital Content Protection And Fair Use: What`s the Use; Journal on Telecomm. & High Tech L. vol. 3, p.428

subject matter that the Member States are not entitled to introduce. In Article 6 (2) is given only a guideline providing the concept of the adequate legal protection of the effective technological measure.

- The *public* policy exceptions are different from those that take place according to the *private* copying exceptions in EU copyright Directive. The exception of private copying is not mandatory, while the public policy exceptions are.
- Also, the public and the private copying exceptions do not apply the material provided through any interactive on-demand service as it is provided by the Recital 53 of the Directive.

4 CHAPTER 4 . The interoperability issue

The position of the DRM in the legal system, its part in the world of intellectual property and its ability to provide solutions for the society are some of the main topics of this chapter.

In the context of DRM, interoperability is based on the multiple ability of systems, devices and applications to work together under the customer`s control. Hence, for the user this indicates the flexibility to choose among different services that offer DRM-protected content, which in turn can be used with different applications or on different devices. From the perspective of the content provider it means that content and rights can be cleared once and distributed over the most efficient distribution channel, without being locked. For the distributor of the content, DRM interoperability ensures that its technological choice is not going to affect the utility of its service for the users, as the delivered content might be played by any application and device.[39]

The incentives of the content industry to deal with the idea of flexible and interoperable DRM systems are not so influential in the online environment of copyright in our days. The main barrier is the competitive environment of the digital rights management mechanisms. Also, the lack of standardization of the DRM systems is a consequence of this competitive environment that characterizes the distribution of copyrighted content online. The private use of this content with flexibility, in many devices and applications, distinguishing the personal and the public use, as it happens in the music industry, could reduce the attempts of circumvention of DRM systems and increase the demand for the content, based on interoperability. As a result, the benefits to innovation could be multiple since relevant industries are given the access and tools to develop such technologies.

The key factor from which the right management systems can benefit from in Web Services (WS) is modularity, a component or building block, mostly used to build larger ser-

---

[39] Urs Gasser & John Palfrey: DRM-protected Music Interoperability and Innovation, Berkman Publication Series 6 (Nov. 2007), as is cited in the article DRM Interoperability, by Hiram Melendez- Juarbe, B.U.J.SCI. & TECH. L. VOL 15 , II B.

vices. The actual platform that comprises the term WS is achieved by several technologies and the core ones among them are the HTTP and XML. The former is a well- established, ubiquitous protocol found behind the World Wide Web while the latter is a very powerful semantic mark-up language that enables the accurate description of any content[40].

The online entertainment company in the United States, Netflix, allows users to stream films and television series on their computer. The users pay a monthly fee which allows them access to the online content provided by Netflix which is online available to customers. The DRM established by Microsoft, has been fully interoperable with Netflix streaming technology, and Apple`s too, even the latter was not compatible at the beginning. This is a real scenario, presenting the importance of interoperability, in particular, in the entertainment industry. Also, the software used in this case has a crucial position in interoperability and in competitiveness between the colossal enterprises of the IT sector. Moreover, no barrier has been set but it seems like the decision of one of the players not to interoperate with a specific system in the online environment, creates an actual barrier.

A question arises regarding the consequences of lack of interoperability and its aftermath in regards to the consumer. How is the consumer affected by the launching of systems that their platforms do not support?

In essence, the end-user faces a limit of the uses that can be achieve online, regarding the content that has been acquired in this particular environment, because of the imposed control over it by a DRM system. Of course, with the help of the DRM the copyright holders can extend their influence to their digital content used for private and personal reasons, in a way that differs from the analog world. But, at the same time, the dominant technology firms have a tendency to increase their competition in order to establish a DRM regime and get the benefit of the provision of the basic technological platform which could affect the whole perception of the DRM mechanism online. The user`s experience under these circumstances is affected by some limits when he/she attempts to experience digital products and acquire information.

---

[40] Serrão Carlos and others, i-DRM - interoperable Digital Rights Management, VDM, p.100

The technological development in regards to the digital environment and the content available has created a, rather new, regime where the copyright owner is able to control the access reachable by the users and their ability to make copies, play games or edit a work in private. In fact, we, probably, become "*less and less a free culture, more and more a permission culture*[41]*."* The fear of Lessig, gives an aspect of the copyright online and the enactment of sophisticated DRM systems in order to protect the valuable content.

4.1 The legal provision of interoperability

For consumers and competitors DRM interoperability is of significant importance. Today, DRM systems in the market do not trust one another and rely on proprietary license formats and protocols. There is no general mechanism for secure content interchange between systems, which are not equally expressive, in particular in US and EU. Also, the DRM systems are still evolving; with the latest example being the encrypted mechanism in HTML5. The EUCD lacks a clear provision of interoperability and the level of the development and marketing of devices that tend to be compatible.

The Copyright Directive in its Recital 54 does not impose any obligation to Member States for the concept of interoperability to be achievable:

"…*differences between technological measures could lead to an incompatibility of systems within the Community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems*."

The inclusion of the term i*nteroperability* sounds like a recommendation in the wording of the Directive, probably because in the time of the enactment of Copyright Directive, the technology did not achieved so much in the DRM sector and interoperability was not a major issue in the copyright world. On the contrary, in telecommunications law and regulation in EU, the concept of interoperability and interconnection was specifically defined in Access Directive. In Recital 48 of EUCD it is also noted that the DRM systems should not

---

[41] Lawrence Lessig, Free Culture, The Penguin Press,2004,pg.8,par.3

prevent "the *normal operation of electronic equipment and its technological development."* Under these provisions it is obvious that the DRM has to be used in order to allow compatibility without any kind of permission and authorization of a DRM provider.

The constraint that Article 6 (2) provides to the circumvention of a DRM of devices, for example, , leads to the hypothesis that in case that one wants to launch in the market a device that encloses a series of encrypted files under a specific DRM standard, has to:

- Define that the technical structure of the compatible device does not fall in the EUCD`s provision of anti-circumvention devices
- Explain that the requirements of Article 6 (2) (a), (b), (c) are not fulfilled.

The interoperability issue was, already, a reality in the software world at the time the Software Directive was implemented[42]. The scope of the provision was broadened and the Recital 23 of this Directive introduced the aspect that the interoperability provision covers not only interfaces towards other "pure" software components but also interfaces towards any system component from other manufacturers that should "work together" with the software component. So, the provision "*is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together*".

Since software components can in many cases be replaced by hardware components, an opposite interpretation would imply a significant reduction in the scope of the interoperability provision[43].

---

[42] Council Directive 91/250/ECC of 14 May 1991, on the legal protection of computer programs.

[43] Mikko Valimaki and Ville Oksanen, DRM Interoperability and Intellectual Property Policy in Europe, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261643

4.2 Interoperability and Consumer Protection Law

When a company tries to involve potential consumers using DRM, the consumer protection law may apply. The intervention of national consumer protective authorities in EU is provided under the Directive 93/13/EEC of 5 April 1993, on unfair terms in consumer contracts. An early important case in Europe was one that took place in Norway, when the Norwegian Consumer Council filed a complaint with the Consumer Ombudsman against iTunes Music Store Norge in January 2006. The unfair fact was that the music bought on Apple's iTunes Store could only be reproduced on iPods.

The Consumer Council and Consumer Ombudsman criticized Apple`s interoperability policy but Apple was not in a position to compromise. In 06.01.2009 Apple opened up iTunes Store without DRMS putting an end to the case[44]. A recent case in the US has shown that DRM issues involving Apple are still in progress[45] , while they have an impact to consumers and anti-trust legislation. In practice, DRM can increase the power of rights holders in setting excessive conditions on the users in the digital environment. There is a combination of secure distribution for payment, monitoring and management for protected content with a sophisticated automated system under a contractual basis. This could increase the power of rights-holders over the material and the end-user.

The DRM *ex ante* could impose unilateral terms and conditions. For example, in the case of a software company, which writes the End User License Agreements restricting the rights of its customers to transfer and use its products. Usually, in this case the extended use of the so-called click-wrap agreements is notable. So, the issue arises when a contract is not the result of a negotiation between parties, but a form of defined terms and conditions unilaterally. According to the Bureau Europeen des Unions de Consommateurs (BEUC), the current course of DRM development "*seems to aim at creating a new relationship between right holders and consumers, with altered consumer rights, freedoms and expecta-*

---

[44] http://forbrukerportalen.no/

[45] Case4:05-cv-00037-YGR Document788 Filed 09/26/14

tions and towards the general replacement of copyright law with contract law and codes.[46] ,,

4.3 The contract and the DRM

The contract structure in the DRM environment is similar to a standard form contract, having the power to enforce restrictive terms of service conditions deactivating the reselling of the digital content and not supporting business models related to the exhaustion principle and first sale doctrine. The standardized contract terms are those the DRM systems support even though the market can create private copyright protection through contract. Copyright law is able to set a standard of consumer protection even if it is not the priority of copyright law to protect the consumers. Some concerns for the consumer interests includes Article 6 (4) of the Copyright Directive because it provides these interests by encouraging right-holders to adopt voluntarily any necessary measure to make the means of benefiting from exceptions or limitations available to beneficiaries.

What interests the consumer of an online service or product is the nature of the contract regarding the DRM. The use of DRM in a contract could lead to replacement of the consumer rights under copyright law by a commercial agreement between the contractual parties. This can have as a consequence the modification of the balance of rights.

The legal right of the consumer under the copyright law, which is to copy for a private use a specific material online, could be illegal if the material is protected by a DRM system and restricted under the contract law and the relative agreement. The implementation of intellectual property rights is not a case of simple private agreements affected by private law. It is rather critical to be mentioned in the contractual obligations of the end-user the limit of the content use according to copyright principles. The online agreements that are supervised and monitored by DRMs could modify the balance of rights between right holders

[46] As cited in: Nicola Lucchi, Digital Media & Intellectual Property, Springer , 2006, Chapter 3, p.108, par.2

and consumers. There is an actual danger of treating as law the defined code, which is the DRMS based on.

When a DRM is seen as a contract, it could be used to protect content that is not subject to intellectual property rights protection and could erect barriers not only at the entrance level[47]. If the DRM and its REL does not know when a copyright term expires, it sets an exit barrier by having the same control on works that should exit copyright and obstructing their entry into the public domain. That has as a consequence the establishment of a copyright protection without an end.

4.4 Copyright law and contract law: The distinction of license and sell

Some kind of confusion could be caused when the identification of an online contract falls between the distinction of a license and a sale. In the case of a license, the treatment of the agreement falls under the contract law and in the case of a sale, under the copyright law. Since, under the license agreement the vendors avoid the exhaustion right it is preferable among them. It is easier under these licensing conditions for limitations to be imposed to the use of content. The doctrine of lacking of conscience in common and continental law provides the duty of the courts to define a contract's conditions as well as if that contract is fair or not. The contract formation and copyright practices do not seem well examined under this doctrine because their effects are not standardized and measurable in the online market.

The EU legal framework provides a series of rules unified in the European Community Council Directive on Unfair Terms in Consumer Contracts[48]. The Unfair Term Directive recognizes the invalidation of terms that are standardized and are the cause of significant imbalance of obligations between the parties to the loss of the consumers. According to Article 3 (1) "A *contractual term which has not been individually negotiated shall be re-*

---

[47] As cited in Nicola Lucchi, Digital Media & Intellectual Property, Springer , 2006, Chapter 3, p.104

[48] Council Directive 93/13/EEC of April 1993 on unfair terms in consumer contracts

garded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties` rights and obligations arising under the contract, to the detriment of the consumer". The Annex, also, of the same Directive includes a list of unfair terms. The baseline is set as a minimum to the Member States which their national consumer legislation will define the concept of *unfairness* in a contract. The unfair term has to produce a significant imbalance in the rights of the parties causing the detriment of the consumer, especially if such a term exists in a standard form contract which can include a DRM system. The TPM can follow technical instructions which cannot include any validation system of the terms of a contract. This can be a disability of a DRMS and could cause implications during the access of a copyrighted material online.

The Electronic Commerce Directive [49], also, requires the exchange of certain information about the information of on-line suppliers to consumers about the identity of the supplier, the qualifications of its products and the terms and conditions of the contract formed online in order to be valid that particular contract[50]. The exchange of information online has the risk of exposing personal data to a potential hacking activity, including the lack of security standards of a DRMS.

The Distance Contract Directive[51] provides to consumers the right to withdraw from a contract when the contract formation takes place without physical presence of both contractual parties[52]. The consumer must have received a written confirmation of the contract, capable to be stored in a durable medium at the time of the performance of the contract. The DRMS implementation has to take into account the storage of information. Cloud computing is a point of serious consideration regarding this point.

It is crucial to be found remedies to protect the consumer`s rights deciding if all content rights transaction is about to fall under contract instead of copyright law. The application of

---

[49] Council Directive 2000/31/EC, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

[50] Articles 5 and 10 of E-Commerce Directive

[51] Council Directive 97/7/EC , on the protection of consumers in respect of distance-contracts

[52] Article 6, Distance Contract Directive.

general consumer protection law could immediately offer an effective solution to reduce any balance between parties.

The EU Commission believes that markets will define an open and non- discriminative DRM[53] standard while the interoperability policies are matter of national law, according to EUCD. The statement is as follows: "*A prerequisite to ensure Community- wide accessibility to DRM systems and services by right holders as well as users and, in particular, consumers, is that DRM systems and services are interoperable".*

In EU, the case law gives an example regarding the licensing and selling of copyrighted material in the online world: In the case *Used Soft GmbH vs. Oracle International Corp*.[54], the ECJ recognized that the license of a software product can be resalable. The Court based to Article 4 (2) and 5(1) of EUCD, stated that in the event of the resale of a user license and that license having originally been granted by the right holder, the second acquirer of the license will be able to rely on the exhaustion of the distribution right and benefit from the right of reproduction provided for in the relative provision. The EU decided to cover the digital form of transmission under the *making available right*. Article 3(3) EUCD states that this right is not subject to exhaustion.

In the US has been chosen to be implemented the right of *making available* of Article 6 WCT, not as a separate right, but incorporating it into the distribution right to which exhaustion applies[55].

---

53 Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee. The Management of Copyright and Related Rights in the Internal Market, COM/2004/0261, final.

54 Case: ECJ C-128/11 Used Soft GmbH vs. Oracle International Corp.

55 Cimentarov Petar: The Exhaustion of Copyright in the Digital Environment: Are the Rules Suitable to Deal with Digitally Transmitted Goods? A Comparative Approach between the USA and the EU, at http://buck.ugent.be/fulltxt/RUG01/001/786/979/RUG01-001786979_2012_0001_AC.pdf

4.5 DRM standardization and interoperability

Standardization is essential in establishing the economies of scale that will make digital content and IP distribution a viable and profitable business. Non-standardized consumer services almost always cause excessive market fragmentation that usually do not allow for an economy of scale to evolve, thus resulting in uneconomical demand.[56]

In EUCD the standardization provision is rather an affirmation of the importance of the related to standardization aspects of technology, in order to protect the digital copyrighted work. Recital 54 provides that:

"Important progress has been made in the international standardization of technical systems of identification of works and protected subject-matter in digital format".

The DRM interoperability discussion has settled around the REL technologies, with the well-known amongst them being the extensible Rights Markup Language (XrML), now included in MPEG-21. Some modules of MPEG platforms are standardized by the International Standards Organization (ISO).

A successful DRM standard includes clarified goals and applications and evaluation of the content and its security requirements. Also, is necessary the balance between interoperability and entrepreneurship. There is the possibility in the market for the consumers to prefer a particular product over others and in that case we could have a *de facto* standard. It seems that the current lack of interoperability in the DRM context is due in large part to a standards war. It is usual to see the sponsor of an incumbent technology opposing interoperability while entrants can be seen as favoring interoperable standards[57]. This could explain the different DRM systems of Apple and Microsoft, for example.

---

[56] Spencer Cheng, Avni Rambhia, DRM and Standardization- Can DRM Be Standardized; E. Becker et al.: Digital Rights Management, LNCS 2770, PP.162-177,2003

[57] Hiram Melendez- Juarbe, DRM Interoperability, B.U.J. SCI & TECH. L. Vol. 15,p.30

Three types of ways in which standards can be developed, are described by Mark Lemley:[58]

- The *de facto* standards, as the result of competition in network markets
- In the case of the imposition after a government inquiring, in order to follow all market participants its specifications. The digital TV in US is an example.
- Another approach to achieving interoperability is through private standard- setting organizations composed of key market players.

Because of the competition in online market and applications, the likelihood of a single interoperable standard lessens and so far there is not a flexible and reliable system concerning the standardized interoperability regarding the DRM systems. Somehow, the consortia of vast content providers under the HTML 5 application seem to create a de facto DRM standard, unifying a number of different sub-systems. The aspect of a new ecosystem is enforced by the HTML 5 platform by the time it is used as a base for a broad accepted standardization.

5 CHAPTER 5. THE CASE OF HTML 5

The World Wide Web Consortium (W3C) is an international community where Member organizations and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee, its mission is to lead the Web to its full potential[59]. W3C standards define an Open Web Platform for application development that has the unprecedented potential to enable developers to build rich interactive experiences, powered by vast data stores that are available on any device. Although the boundaries of the platform continue to evolve, industry leaders speak nearly in unison about how Hypertext Markup Language 5 (HTML 5) will be the cornerstone for this platform[60].

---

[58] Ibid, p.32
[59] http://www.w3.org/Consortium/
[60] http://www.w3.org/standards/

The Open Web Platform is the collection of open (royalty-free) technologies which enables the Web. Using the Open Web Platform, everyone has the right to implement a software component of the Web without requiring any approvals or waiving license fees[61]. The W3C in the Editor`s Draft of 24 October 2014[62] led to a Recommendation, a term for a final and complete specification, of 28th of October 2014 regarding the Application Programming Interface (API) ,which specifies the software component in terms of the operations of computer programming. "*The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors."*

The Working Draft of May 10th 2013 on Encrypted Media Extensions (EME) raised serious criticism about the intentions of 3WC to transform HTML 5 to some kind of online Panopticon[63].

"The API supports use cases ranging from simple clear key decryption to high value video (given an appropriate user agent implementation). License/key exchange is controlled by the application, facilitating the development of robust playback applications supporting a range of content decryption and protection technologies. This specification does not define a content protection or Digital Rights Management system. Rather, it defines a common API that may be used to discover, select and interact with such systems as well as with simpler content encryption systems. Implementation of Digital Rights Management is not required for compliance with this specification: only the Clear Key system is required to be implemented as a common baseline[64]."

The Recommendation of the 28th of October 2014 defines the specifications of the core language of the World Wide Web (WWW): the Hypertext Markup Language (HTML). The

---

[61] http://www.w3.org/wiki/Open_Web_Platform
[62] https:dvcs.w3.org/hg/html-media/raw-file/tip/encrypted-media/encrypted-media.html
[63] The concept of continuous surveillance was first introduced by Jeremy Bentham during the 18th century. As a metaphor the idea was used by many authors and philosophers, amongst them by Michael Foucault in his book *Discipline and Punish* (1975).
[64] Ibid, in the Abstract

new features are introduced in order for authoring practices to prevail and define clear criteria for user agents in an effort to improve interoperability[65].

The concerns of the European Commission regarding the scope and functioning of copyright and related rights associated with internet transmissions in the Single Market and the exceptions and limitations granted under the EUCD are carried out after an "*in-depth legal and economic analysis*[66]*"*. Also, "*technology, the fast evolving nature of digital business models and the growing autonomy of online consumers, all call for a constant assessment as to whether current copyright rules set the right incentives and enable right holders, users of rights and consumers to take advantage of the opportunities that modern technologies provide*." The monitoring of the use of licenses should respect fundamental rights, namely to respect of private and family life and data protection[67]. The HTML 5 is an effective means which provides the interoperability with other online platforms and applications in order to be detected copyright infringements of copyrighted material.

5.1 The criticism

The decision of W3C started a discussion regarding the threat to the concept of Open Web that could cause a potential DRMS encrypted in HTML 5. The Electronic Frontier Foundation (EFF) as a full member of W3C, made a formal objection to W3C regarding the DRM in HTML 5, claiming that the proposal defines a new `black box` for the entertainment industry, fenced off from control by the browser and end-user. According to the EFF[68] , DRM standards look like normal technical standards but turn out to have quite different qualities. The reason for the aforementioned is that the EME chills the speech of technologists, lock down technology and violate property rights by seizing control of personal computers from their owners.

---

[65] http://www.w3.org/TR/html5/
[66] Proposal for a Directive of the European Parliament and the Council on collective management of copyright, Brussels,11.7.2012, COM(2012) 372 final, par 1.2
[67] Ibid, Recital 27
[68] https:www.eff.org/press/releases/eff-makes-formal-objection-drm-html5

The EME, notes EFF, can lead to a Web where images and pages cannot be saved or searched, advertisements cannot be blocked and innovative new browsers cannot compete without explicit permission from big content companies. Another explicit fear is that the adoption of the proposal could create serious impediments to interoperability and access for all.

The W3C was criticized by the EFF for lacking development of a policy regarding DRM and the proposal has to be seen as a constraint to open source developers, to competition and interoperability. It is, also, locked in legacy business models, which opposes innovation and the fair use model that created the Web.

Following the same direction to criticism, Cory Doctorow[69], noted that the potential DRM to the HTML 5 standard, will have incompatible effects on the W3C`s most important policies. Comparing DVDs to CDs, writes, CDs had no DRM, so it was legal to invent technologies like the iPod and iTunes, which transcoded and copied music for personal uses. DVDs featured DRMs, so it was illegal to add any features to them , and in the nearly 20 years since they were introduced, no legal technologies that do what iTunes and the iPod did in 2001, have been introduced to the market. According to Doctorow, this is the regime that the W3C stands to add to the Web, and that Berners-Lee has endorsed with his remarks[70]. Mozilla's decision to include in their Firefox browser a closed-source DRM from Adobe was seen[71] as an attempt to produce DRM systems that treat internet users as untrusted adversaries controlled by their computers.

[69] http://www.theguardian.com/technology/blog/2013/mar/12/tim-berners-lee-drm-cory-doctorow
[70] Idem
[71] http://www.theguardian.com/technology/2014/may/14/firefox-closed-source-drm-video-browser-cory-doctorow

5.2 The DRM and the fear of mass surveillance

Copyright along with intellectual property rights more generally are not intrinsically in tension with data protection rights. In their origins, copyright and data protection share common ground in their origins. Doctrines on copyright have been used to help ground to right to privacy and privacy doctrines have been used to help ground aspects of copyright[72]. The conflict that has emerged between copyright and data protection in recent years has centered on demands by IPR-holders to gain access to information and identities of persons considered as engaged to file-sharing activities. The principle of proportionality is a crucial criterion when the legislator and courts in EU attempt to define the balance between the IP rights and the respect to privacy and personal data. Article 8 of European Convention on Human Rights provides the privacy as a fundamental right. The EUCD, in EU legislation, requires sanctions to be *proportionate* in Article 8(1). The CJEU in *Scarlet Extended case*[73], dealt with the lawfulness of a requirement, sought for by IPR-holders, that an Internet Service Provider (ISP) introduce a system for systematically monitoring and filtering all Internet usage of its customers. The Court held that the required system did not offer a fair balance between the rights of ISPs to conduct their business and the end-users rights to privacy and data protection along with their rights to freedom of expression. There is a necessity of clear and predictable legal authority for a system of online surveillance involving the ISPs to be permitted. This necessity for legal authority is springing from Articles 8 (2) and 10 (2) of ECHR. The interference by the state, in any case, must be in accordance with the law. This means that there must be a basis in law in order to be justified the interference and the ideals of "rule of law" must be satisfied, as well.[74]

The fear of mass surveillance, expressed by commentators and scholars, has not been realized in practice. The Sony Rootkit case in US in 2005 raised a number of concerns in

---

[72] Bygrave A. Lee, Data protection vs. Copyright,Internationalization of Law in the Digital Information Society: Nordic Yearbook of Law and Informatics 2010-2012, Ex Tuto, 2013, pg.56

[73] Case C-70/10, Scarlet Extended SA vs SABAM

[74] Idem,pg.72

security, privacy and consumer protection issues after the installation of Sony`s BMG root-kit in a number of discs, running on Windows operating systems. A rootkit is a type of software designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer. The Sony BMG CDs included software called Extended Copy Protection with copy protection and DRM. After the rootkit reveal by a software engineer, the company recalled it. Numerous class action lawsuits were filed and Sony BMG agreed to a settlement[75].In Europe, the so-called Greek wiretapping case[76] in 2004-5 involved the illegal tapping of more than 100 mobile phones on the Vodafone Greece network, belonging mostly to members of the Greek government. Erickson switches were imposed to these phone rootkits, monitoring illegally the mobile calls. At the end, the Hellenic Authority for the Information and Communication Security and Privacy fined Vodafone with 76 million euros.

The use of DRM devices is not popular by current companies. The major change to their preferences is reflected to applications like HTML 5, creating an ecosystem with specific technical features.

5.1 Is there a real threat for Open Web by the HTML 5 DRMS?[77]

The EME does not specify *per se* any DRM scheme. It defines a set of APIs that allow Java and HTML to interact with decryption/ protection modules. These modules will tend to be platform specific in one way or another and will contain the core DRM technology. Practically, there are important companies working on the specifications (as Netflix,

---

[75] http://w2.eff.org/IP/DRM/Sony-BMG/settlement_faq.php#1

[76] http://spectrum.ieee.org/telecom/security/the-athens-affair

[77] Most of the information is from http://arstechnica.com/business/2013/05/drm-in-html5-is-a-victory-for-the-open-web-not-a-defeat/

Google, Microsoft) in order to be built a common DRM platform. The users of EME, like Netflix, are already streaming DRM-protected media, so it is not of much importance if browsers implement W3C EME or non-W3C EME when the technology and its capabilities are identical.

Under the current model, whether it is DRM-capable browser plugins or DRM-capable apps, a distributor such as Spotify, for example, have no reason to experiment with unprotected content. Users are already using a DRM-capable platform and they are unlikely to even notice if some of the songs are unprotected. It would not make any difference to them and that would not be the case if Netflix or Spotify used an HTML 5 distribution platform built on top of EME. That would be the case, because users will not have access to EME either because their platform is not suitable with a DRM module or because the DRM modules could be disabled.

An application outside the EME would probably give companies like Netflix, the opportunity to experiment with unprotected content. The users that are not able to use the protected content could reach the unprotected one after the removing of a DRMS and the potential income could be greater. With EME there is a way for content distributors to check if unprotected distribution is viable. This is a crucial factor that could enforce innovation.

In practice[78], the HTML 5 and W3C will not stop the DRM but the companies shipping DRM can do it, as part of their business activity. DRM already exists in many devices such as in machines running versions of Microsoft Windows with the PlayReady DRM technology. Google works with EME in its Widevine DRM system on Chromebooks and prepared a demonstration of how DRM will work with Youtube[79]. EME is not part of the HTML 5 standard and it is not a DRM system. At the same time, allows HTML to be compatible with existing DRM systems.

---

[78] The Netflix adoption of HTML 5 in Video at http://techblog.netflix.com/2013/04/html5-video-at-netflix.html

[79] Dr Harry Halpin in http://www.theguardian.com/technology/2013/jun/06/html5-drm-w3c-open-web

5.2 Innovation and DRMS

The definition[80] of *innovation* includes the act and the process of introducing new ideas, devices or methods. The Oslo Manual for measuring innovation[81] defines four types of innovation as follows: product innovation, process innovation, marketing and organizational innovation. Now, the DRMS has been criticized as imposing constraints to internet based innovation. However, there are two sides to this coin. In other words, the effects of DRMS on innovation can be either positive or negative. In the context where DRMS could enforce intellectual property rights to a high level, obstructing innovation, there are two main arguments.

Firstly, the DRM systems can jeopardize fair use, first sale and time-limited monopoly rights[82] . The combination of DRM mechanisms and legal tools enable right holders to protect their material in cyberspace in a way that would not be feasible using only the copyright law. The rules of anti-circumvention of devices and DRM software in the EU and US legal structure indicate the concern for online control of copyrighted works without excluding legitimate purposes such as the encryption research.

Secondly, the economic inefficiency of DRMS could be a barrier for new business entries in the market. If a product or system (e.g. Microsoft Windows) sets a specific standard DRM could make the appearance of new competitors more difficult. The low entry barriers of the internet have the potential to attract a whole new set of participants with different preferences to those of classic economic agents, who are able to contribute valuable content and have further implications for innovation[83].The example of the plethora of on-line travel agents like *www.booking.com* and the online presence of a traditional agent, *www.tui.com,* is illustrative.

---

[80] Merriam-Webster Dictionary

[81] http://www.oecd.org/sti/inno/oslomanualguidelinesforcollectingandinterpretinginnovationdata3rdedition.htm

[82] Picot Arnold, Marina Fiedler, Impacts of DRM on internet Based Innovation, in E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 288-300,2003, Springer-VBH

[83] Ibid, pg.295

In addition, DRMS is important in case of costly innovations, like those of the entertainment industry, whereas inventors consider the cost of recovering old works and creating new ones. If there are not secure DRMS to protect the content, expensive films and productions in the digital world, with a very small or without any cost of downloading would not be attractive for investors. Also, without protection mechanisms granting exclusive exploitation rights for a limited period of time there could be a tendency for innovations that are inherently secretive or short-life cycled[84]. Mandatory DRMS benefit the inventors who want an exclusive right and are not useful to those interested in a fast distribution of their ideas and services.

5.3 Innovation and anti-circumvention policies

The DRMS in practice do not stop copying and file-sharing. The impact on scientific inquiry and innovation in product design of the anti-circumvention provisions in EU and US legislation has been noted by a number of scholars. Fred von Lohmann chronicled the `unintended consequences` of anti-circumvention law, particularly in dampening the opportunities to innovate in the complementary markets *around* copyrighted works[85]. DRMS may have the effect of leveraging the copyright-holders monopoly, granted by the law regarding the expression into technological field.

On one hand, the market structure of DRMS can hold back innovation because of the excessive control over the distribution mechanisms regarding the copyrighted works. Potential innovators could find a barrier if they attempt to widen the market of end-users. On the other hand, there is an argument that tying control over copyrighted works could facilitate price and product differentiation[86].

Moreover, the digital environment is ideal for innovative products and services performed by end-users. The internet lessens the costs of communication and provides the exchange

[84] Ibid, pg. 292
[85] As cited in: Wendy Seltzer, The Imperfect is the Enemy of the Good: Anti-circumvention versus Open User Innovation, Berkeley Technology Law Journal, vol.25, 2010, pg. 941
[86] Ibid, pg.942

of information in a minimum- cost way. *Start-up* companies are feasible to set up enabling end –users in novelty and innovation. The popularity of free and open source software attracted the interest of user communities in improving and modifying services and products in cyberspace. The involvement of the user in the innovative procedure has a direct impact on social welfare and increases social value, even if the approach is not based on an organized infrastructure.

Lastly, the direct involvement of the end-users to an innovative attempt can contribute better and, sometimes, customized solutions in the market, because are able to respond to changing needs. This may have an indirect impact to commercial innovation and large firms can benefit from the expansion of information regarding the effectiveness of their products online. The process of innovation itself is rewarding the user-innovator. Also, it offers intellectual stimulation and development of new skills in the community and engagement of the same community with technology[87]. Anti-circumvention sends a message to developers and both, commercial and user- innovators that certain activities and opportunities are off limits. Even if it is technically feasible to improve interoperation with a wide variety of media, for example, they are forbidden from doing so without advance permission[88]. If the code in DRMS is treated as a law, side effects are caused to innovation, as well. Potential innovators, in that case, are possible to be confused regarding the actions that are allowed or not to be performed when they attempt to improve services and applications in a digital environment.

[87] Ibid, pg. 968
[88] Ibid, pg. 972

6 CONCLUSION

All in all, the concept of DRMS is connected to the digital world and the expansion of copyright-protected works in cyberspace. Hence why, it is a necessity for copyright holders even if it is not effective in preventing piracy and file-sharing in a large scale. The DRM introduced some new concepts like the *circumvention* of devices and software, becoming part of the legislation worldwide as a global phenomenon. This "globalization" affected, on one hand, the well-established principles in the intellectual property protective rules and on the other, the personal data security, innovation and interoperability of services and products in the electronic environment. The enforcement attempts of the online right-holders have been provided in order to be adequate in the face of the EU legislation. Also, the judicial systems have to evaluate the relative factors of right *exhaustio*n or *first sale* following either a case- by- case approach or a specific definition of permitted usages. Hence, the courts have to face the nature of DRM as a functionality based one on the *ex ante* programming of access to the protected work online.

The EU legislation in EUCD set the circumvention prohibitions as having a *de facto* unlimited character. The CJEU, in my opinion, in the Nintendo case, offered some useful guidelines in order to clarify the prerequisites of a permitted circumvention of a DRM device and application, considering the principle of proportionality and introducing relative qualitative and quantitative criteria. The concept of interoperability in the same case becomes more specific, compared to the provisions of EUCD. The case law, in fact, gives the judicial systems of the Member States legal tools to proceed in case-by-case examinations regarding the DRM applicable law. In Nintendo case, was determined that there is unlikely to be any justification for protection of TPMs which prevent or limit acts outside of the authorization of a right-holder. This case can establish the boundaries for the TPMs used in software and digital media industry. The law becomes part of the new ecosystem of DRMS under the provisions of the decisions of CJEU.

The future cases in CJEU will have a solid base, after the Nintendo case, to interpret the influence of the interoperability of DRM platforms and the impact of such mechanisms to privacy, innovation and the exhaustion principle.

The importance of consumer protection regarding the online formation of contracts and agreements is an issue that DRM has to deal with effectively. The applicable law related to these contracts is not so clear, because there is a difference between sale and online license in the way these two actions are treated by the law.

In addition, many concerns have arisen relating to personal data protection and relative data flow to third countries and processors, outside the EU. The expansion of new mobile devices, the speed of information online and the elaboration of data by DRMS threat the concept of privacy and data security, exposing personal data to potential dangers.

To conclude, the Digital Rights Management Systems are here to stay. The DRMS implementation challenges a series of concepts in the intellectual property world. Some of the effects that have been noticed are the *exhaustion* and *first sale* principles, noted in the Berne Convention, the *fair use* doctrine in the United States' DMCA and the treatment of the code as law. Also, in DRM, issues regarding privacy, personal data and system interoperability are of high concern for the consumers. The DRM mechanisms are able to have an impact on the innovative spirit in society, when they act as constraints to reverse engineering and within the limits of anti-circumvention legislature. The interests surrounding the controlling of the copyrighted material online are immense and the lobbying by content providers in international organizations is extensive and ever present. The technology related to DRMS has already moved into new formats such as "cloud"-based computing and the speed at which legal rules move behind the development of such technological achievements is rather low.

The DRMS are in a transitional phase. Technologies like the encrypted mechanism in HTML 5 or the Ultraviolet, regarding the digital discs, work partly as DRMS, having the ability to interoperate with other systems in an electronic environment in order to achieve the main goal of controlling copyrighted material. The new concept of DRM tends not to create devices and services that could be bypassed easily, but rather prefers to introduce end-users to an ecosystem where personalization and interaction are fundamental in the distribution system of the protected works. The position of the HTML 5 in this ecosystem has some new characteristics. Without being *per se* a DRMS, it is a platform where browsers can impose their DRM mechanisms. This, looks like a compromise between the content

providers and the negative perception of the DRMS by the consumers in society. However, it is not the compromise it seems to be. The effectiveness of the DRMS under this perspective has definitely increased because, presently, it can be part of the way that information is exchanged online. Legal risks concerning personal data and innovation are, also, increased due to the aforementioned reasons.

Finally, the evolutional character of the DRM technology is leading to more sophisticated mechanisms that could monitor any individual`s activity online. That is a reason why the controversial presence of the DRMS in the intellectual property world increases the responsibilities of lawmakers to confront the challenges the future might bring. The future of DRMS is connected to implementations like HTML 5, their deployment by content providers, their standardization and their impact on a governance model of member-driven organizations, like W3C. Fundamental concerns for the side effects of the future DRMS on the idea of an Open Web, will continue to characterize the online content control mechanisms.

Table of References

Books

Asoke K. Talukder, Manish Chaitanya: Architecting Secure Software Systems, CRC Press, 2008

Becker Eberhard, Buhse Willms, Gunnewig Dirk, Rump Niels (Eds.): Digital Rights Management, Technological, Economic, Legal and Political Aspects, Springer, Berlin, 2003

Bygrave A. Lee: Data Privacy Law, An International Perspective, Oxford, 2014

D. Wright, P. De Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, Springer, 2012

David Matthew: Peer to Peer and the Music Industry, the Criminalization of Sharing, SAGE, 2010

Herman D. Bill: The Fight Over Digital Rights, the Politics of Copyright and Technology, Cambridge University Press, Cambridge, 2013

Kindt J. Els: Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis, Springer, 2013

Klitou D.: Privacy –Invading Technologies and Privacy by Design, Information Technology and Law Series, ASSER PRESS and the author, 2014

Lessig Lawrence, Code V2, online, under the Creative Commons Attribution, at http://codev2.cc/

Lessig Lawrence: Free Culture, The Penguin Press, New York, 2004

Lucchi Nicola: Digital Media & Intellectual Property, in particular chapter 3, Springer, 2006

May Christopher: Digital Rights Management, The Problem of Expanding Ownership Rights, Chandos Publishing, 2007

Millard Christopher, Cloud Computing Law, Oxford University Press, 2013

Patry William: How to Fix Copyright, Oxford University Press, 2011

Petkovic Milan, Jonker Willem (Eds.): Security, Privacy, and Trust in Modern Data Management, Springer, 2007

Schollin Kristoffer: Digital Rights Management, The New Copyright, Jure Förlag AB, Stockholm, 2008

Serrão Carlos, Delgado Jaime, Dias Miguel: iDRM-interoperable Digital Rights Management, Interoperability Mechanisms for Open Rights Management Platforms, VDM Verlag Dr. Müller, Munster, 2009

Stevens Luke, Owen RJ: The Truth About HTML 5, in particular, chapters 10 & 12, Apress, 2013, at http://download.springer.com/static/pdf/366/bok%253A978-1-4302-6416-3.pdf?auth66=1415102428_7b4975b323b824d68aa989fa5b9898eb&ext=.pdf

Weber H. Rolf, Weber Romana: Internet of Things, Legal Perspectives, Springer, 2010

Articles

Benczek Alexander Pius: Implementation of DRM Systems under the EU Legal Framework, in S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, pp.72-94 , Vieweg, 2006.

Bygrave A. Lee, Privacy and Data Protection in an International Perspective, Stockholm Institute for Scandinavian Law & Lee A. Bygrave 2010 in www.scandinavianlaw.se/

Bygrave A. Lee: Data Protection vs. Copyright, in Svantesson B. Jerker Dan & Greenstein Stanley (editors): Internationalization of law in the Digital Information Society, Nordic Yearbook of Law and Informatics 2010-2012, available at http://ssrn.com/abstract=2350131

Bygrave A. Lee: Digital Rights Management and Privacy-Legal Aspects in the European Union in E. Becker et al. (Eds.), Digital Rights Management, pp.418-446,2003, Springer, 2003

Bygrave A. Lee: The Technologication of Copyright: Implications for Privacy and Related Interests, in European Intellectual Property Review, 2002, Vol. 24, no.2, pp. 51-57

Bechtold Stefan: From Copyright to Information Law-Implications of Digital Rights Management, in Security and Privacy in Digital Rights Management, Lecture notes in Computer Science, 2002, at http://link.springer.com/chapter/10.1007/3-540-47870-1_14

Cheng Spencer, Rambhia Avni: DRM and Standardization- Can DRM Be Standardized? , in E. Becker et al. (Eds.): Digital Rights Management, pp. 162-177, Springer, 2003

Cimentarov Petar: The Exhaustion of Copyright in the Digital Environment: Are the Rules Suitable to Deal with Digitally Transmitted Goods? A Comparative Approach between the USA and the EU, at
http://buck.ugent.be/fulltxt/RUG01/001/786/979/RUG01-001786979_2012_0001_AC.pdf

Cohen E. Julie: DRM and Privacy, Berkeley Technology Law Journal, Volume 18, Issue 2, March 2003

Davidson Michal, Gudes Ehud and Tassa Tamir: Efficient and Enhanced Solutions for Content Sharing in DRM Systems, in Atluri V. and Pernul G. (Eds.), DBSec 2014, IFIP

De Wolf & Partners, Study on the legal framework of text and data mining (TDM), Jean-Paul Triaille, lecturer, University of Namur, March 2014

Dr Barker R. George: Agreed Use and Fair Use: The Economic Effects of Fair Use and Other Copyright Exceptions, Paper presented to the 2013 Annual Congress of the Society for Economic Research ON Copyright Issues, MINES Paris Tech, Paris (France), 9th of July 2013

Dusollier Severine: Fair Use by Design in the European Copyright Directive of 2001: An empty promise, at http://www.cfp2002.org/fairuse/dusollier.pdf

Felix Oberholzer-Gee and Koleman Strumpf, File-Sharing and Copyright, in http://musicbusinessresearch.files.wordpress.com/2010/06/paper-felix-oberholzer-gee.pdf

Fernandez Ben: Digital Content Protection and Fair Use: What`s the Use?, Journal on Telecomm. & High Tech. I., Vol. 3, 2005

Gasser Urs and Palfrey John: DRM- protected Music, Interoperability and e- Innovation, Case study at http://cyber.law.harvard.edu/interop

Gnesi Stefania, Matteucci Ilaria, Moiso Corrado, Mori Paolo, Petrocci Marinella and Vescovi Michele: My data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data, in Preneel B. and Iconomou D. (Eds.), pp. 154-171, Springer, 2014

Gomes Nuno Norberto de Andrade: Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights, in Hubner- Fischer S. et al. (Eds.): Privacy and Identity 2010, pp. 90-107, IFIP 2011

Guibault Lucie: Evaluating Directive 2001/29/EC in the light of the digital public domain, International Conference on Public Domain in the Digital Age, Louvain, 2008

Juarbe- Melendez Hiram: DRM Interoperability, at http://www.elplandehiram.org

Koops Jaap- Bert, Leenes Ronald: Code and the slow erosion of Privacy, at http://www.mttlr.org/voltwelve/koops&leenes.pdf

Lohmann von Fred: Fair Use as Innovation Policy, 2008, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1273385

Mazziotti Giuseppe: Freedom of use vs. DRM Technology, at http://download.springer.com/static/pdf/630/chp%253A10.1007%252F978-3-540-75985-0_7.pdf?auth66=1415103812_361b0b936c5b6a739e87d5fcaf0aff7e&ext=.pdf

Munier Manuel, Lalanne Vincent, Pierre-Yves Ardoy and Ricardi Magali: Legal Issues About Metadata Data Privacy vs Information Security in Garcia Alfaro et al. (Eds.): DPM and SETOP 2013, pp.162-177, Springer, 2014

Nimmer David: A Riff on Fair Use in the Digital Millennium Copyright Act, University of Pennsylvania Law Review, VOL. 148, January 2000

Picot Arnold, Marina Fiedler: Impacts of DRM on internet Based Innovation, in E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 288-300, 2003, Springer-VBH

Reidenberg Joel, Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Volume 76, number 3, February 1998 as cited in http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship
Springer, 2003, pg.230

Rife Courant Martine: The fair use doctrine: History, application and implications for (new media) writing teachers, at https://www.msu.edu/~mcgrat71/Writing/Fair_Use_Rife.pdf

Stuart Habel and co-authors in: If Piracy is the Problem, Is DRM the Answer? Digital Rights Management, Becker Eberhard et al., Springer, 2003, pp.224-233

Valimaki Mikko and Oksamen Ville: DRM Interoperability and Intellectual Property Policy in Europe, 2006, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261643

Wendy Seltzer, The Imperfect is the Enemy of the Good: Anti-circumvention versus Open User Innovation, Berkeley Technology Law Journal, vol.25, 2010

Westkamp Guido: Copyright Reform and Necessary Flexibilities, Published online, Max Planck Institute for Innovation and Competition, Springer, 2014

Zingales Nicolo: Digital Copyright, Fair Access and the problem of DRM misuse, Boston College Intellectual Property and Technology Forum at http://www.bciptf.org

Cases

Europe

ECtHR

Case *S .and Marper vs. United Kingdom*, 4 December 2008, at http://www.bailii.org/eu/cases/ECHR/2008/1581.html

European Court of Justice

Case C-355/12, ECJ, Judgment of the Court of 23 January 2014 (request for a preliminary ruling from the Tribunale di Milano, Italy), Nintendo Co. Ltd and others Vs PC Box Srl and 9Net Srl

Case C-128/11, ECJ, Used Soft GmbH vs. Oracle International Corp.

Case C-70/10, Scarlet Extended SA vs SABAM

UK

Case *University of London Press Ltd. Vs. University Tutorial Press Ltd*, at http://oxcheps.new.ox.ac.uk/new/casebook/cases/Cases%20Chapter%2017/University%20of%20London%20Press,%20Ltd%20v%20University%20Tutorial%20Press,%20Ltd.doc

France

Case *Studio Canal, Universal Pictures Video France and SEV vs. S. Perquin and UFC Que Choisir*, Court of Cassation (1st chamber, civil section), 28 February 2006

United States

Case RIIA Vs Napster, Inc., No. 239 F.3d 1004 (9th Cir.2001)

Case The Chamberlain Group, Inc. Vs. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004)

Case RealNetworks, Inc. vs. Streambox, Inc., 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

Case 4:05-cv-00037-YGR Document 788 Filed 09/26/14

Conventions, Treaties & Legal Instruments

Berne Convention for the Protection of Literary and Artistic Works, of September 9, 1886, the Paris Act of July 24,1971 and its amendment on September 28,1979

European Convention for the Protection of Human Rights and Fundamental Freedoms, November 5, 1950, ETS NO.5, Article 8

O.E.C.D Council on 23rd September 1980, Doc. C (80)58/FINAL

The Trade- Related Aspects of Intellectual Property Rights (TRIPS) adopted in Geneva on December 21, 1996 and included it in the WIPO Copyright Treaty (WCT)

Treaty of the Functioning of the European Union (TFEU), Article 115

WIPO Performances and Phonograms Treaty (WPPT), which entered into force on May 20, 2002.

UN Documents

International Covenant on Civil and Political Rights, GA Res.2200Annex (XXI) UN, Article 17

Universal Declaration of Human Rights, December 10,1948, adopted by the General Assembly Resolution 211(III), Article 12, UN Doc. A/810 (1948)

EU Directives, Directive proposals and surveys

Communication from the Commission to the Council, the European Parliament and the European Economic and Social - Committee The Management of Copyright and Related Rights in the Internal Market, COM/2004/0261 final

Council Directive 2000/31/EC, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

Council Directive 93/13/EEC of April 1993 on unfair terms in consumer contracts

Council Directive 97/7/ EC, on the protection of consumers in respect of distance-contracts

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.

Directive 2002/58//EC of the European Parliament and the Council of 12* July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31st July 2002

Directive 91/250/ECC of the European Parliament and of the Council of 14 May 1991, on the legal protection of computer programs

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

Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access

European Commission, Green Paper on Copyright and the Challenge of Technology, Brussels, 31 January 1989, 3.6.4

Proposal for a Directive of the European Parliament and the Council on collective management of copyright, Brussels, 11.7.2012, COM (2012) 372 final, par 1.2

Proposal for a Directive of the European Parliament and the Council on collective management of copyright, Brussels, 11. 7.2012, COM (2012) 372 final, par 1.2

Study on the implementation and effect in Member States` Laws of Directive 2001/29/EC, Final report, Institute for Information Law, University of Amsterdam, The Nederlands, February 2007, 3.2.1

United States

The United States Digital Millennium Copyright Act (US DMCA), chapter 12, title 17 of U.S. Code, the section 1201

Online resources

http://www.3wc.org

http://www.lessig.org/about/

http://sourceforge.net/projects/openipmp

http://www.doi.org

http://www.mp3.history.com/en

http://www.riaa.com/physicalpiracy.php?content_selector=piracy-online-scope-of-the-problem

Envisional Internet Usage Jan2011, An Estimate of Infringing Use of the Internet, as is quoted in http://www.scribd.com/doc/48336443/Envisional-Internet-Usage-Jan2011

https:www.eff.org/press/releases/eff-makes-formal-objection-drm-html5

http://ec.europa.eu/internal_market/copyright/index_en.htm

http://www.theguardian.com/technology/blog/2013/mar/12/tim-berners-lee-drm-cory-doctorow

http://www.theguardian.com/technology/2014/may/14/firefox-closed-source-drm-video-browser-cory-doctorow

http://arstechnica.com/business/2013/05/drm-in-html5-is-a-victory-for-the-open-web-not-a-defeat/

http://www.theguardian.com/technology/2013/jun/06/html5-drm-w3c-open-web

http://www.oecd.org/sti/inno/oslomanualguidelinesforcollectingandinterpretinginnovationdata3rdedition.htm