The implementation of Digital Rights Management (DRM) by the Information Society Directive: a necessary evil?

Maël FABLET

LL.M in International Business Law

University of Exeter

Under the direction of Dr Katerina SIDERI

September 2007

Contact : maelfab@wanadoo.fr

LIST OF CONTENTS

"*One great virtue of copyright is its balance, one that weighs authors' interests against the need for public access. This balance has withstood, and been shaped by, the test of time and, however incompletely, has won civil obedience through the reasonableness of its command*".

Pr Paul Goldstein (Stanford University)[1].

"*Technology makes it possible for people to gain control over everything, except over technology*".

Dr M. John Tudor (School of Electronics and Computer Science - Southampton)

[1] P. Goldstein. "Copyright and Its Substitutes" *Wisconsin. Law Review* 1997. p.871.

Introduction

1. Definition of Digital Rights Management

Digital Rights Management ("DRM"), also called Electronic Rights Management ("ERM"), is a nebulous expression used to describe the range of technological devices and methods that aims to protect intellectual property rights, and copyright in particular, in the new digital sphere, in "the information society".

A global definition would be to say that DRM is a method used to provide an infrastructure which allows creators of an information product to enforce copyright in their product. Enforcement is mainly done by filtering or classifying certain types of content, by controlling access to information products, by preventing unauthorised copying, by identifying the products and copyrights owners, by ensuring that this identification is authentic and by tracking and reporting access to the contents by different users at different times[2]. DRM is the technical sense given to "*any method of 'wrapping' content in order to achieve one or more access-related objectives*"[3].

Such devices are especially used to control exploitation of works online, where rights management is trickier, and where the risk of infringement is higher. To sum-up, we can say that the ultimate goal of DRM systems is to enforce licences between a content provider and a consumer[4]. However, in a broader meaning, DRM systems could be used to secure electronic transactions, to trace behaviours etc. It is a protean notion whose heart is copyright enforcement.

The legal basis of DRM in Europe is the Information Society Directive of 2001[5] (the "ISD") which defines two different notions within the DRM sphere: technological protection measures ("TPM") in article 6, and rights-management information ("RMI") in article 7. To make an analogy with the scientific classification, if DRM is the genus, TPM and RMI are species[6].

---

[2] Lee A. Bygrave, "the technologisation of copyright: implications for privacy and related interests" *European Intellectual Property Review 2002*, 24(2), p.53.

[3] Michael Flint, Nick Fitzpatrick and Clive Thorne, *a user's guide to copyright* (Tottel publishing 6th edition 2006) p. 464

[4] Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan (Trusted Systems Laboratory - HP Laboratories Cambridge), "If Piracy is the Problem, Is DRM the Answer?" *HPL-2003-110*, May 27th , 2003, p.3 http://www.hpl.hp.com/techreports/2003/HPL-2003-110.pdf

[5] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167 , 22/06/2001 p.10 -19

[6] http://en.wikipedia.org/wiki/Copy_protection

Concerning TPM, article 6(3) provides that it concerns "*any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law* (…)". It is intended to prevent users from performing copyright owners' exclusive rights. It includes technologies like copy protection systems[7], encryption techniques to control access to contents etc.

Concerning RMI itself, article 7 (2) of the Directive provides that it is "*any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive* (...)*, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information*". It concerns all processes of identification of works, by means of serial numbers, digital watermarking[8] etc.

Such definitions reflect a new electronic commerce perspective in copyright, but DRM and TPM in particular existed since a long time before the elaboration of the Information Society Directive.

2. History of DRM

The need to distinguish authenticity from copy first enabled the development of watermarking techniques. It consists in putting an original mark on a work or a good that is nearly impossible to reproduce or falsify. For several centuries it has been mainly used for money bills or official documents, before the creation of digital watermarking which is used for many purposes of identification.

Concerning protection of works themselves, most techniques were aimed at copy control and restriction. Indeed, historically, it has always been hard for authors and other rightholders to make users respect their exclusive right of reproduction. This problem has been highlighted in particular for computer games, where publishers and crackers[9] led technological battles. From the first copy protection on cassette tapes or floppy discs in the late seventies to the complex protection of DVD-ROM and their content nowadays, protection methods have continuously evolved and developed. Different systems have been used to prevent reproduction, like bus encryption[10], names and serial numbers given to the user at the time the software is purchased (e.g. *Microsoft Windows* serial number) or phone activation codes etc.

[7] cf. technical glossary p.72
[8] Idem.
[9] Idem.
[10] Idem.

As crackers appeared to always be a length ahead of them, publishers even began to protect their softwares against reproduction thanks to user-interactive methods. Typically, to launch a program, it was necessary for users to answer a question like the following one: "what is the 7th word on the 6th line of page 37 of the manual?". As crackers did not usually reproduce manuals, they could not even access the software because of this preliminary question.

However, what was possible for softwares, where a computer is needed to play and use the content, was not necessarily adequate for music or video. Indeed, softwares keep users in a digital or electronic sphere: it is impossible to use them or copy them without digital equipments. So, users need to electronically decipher softwares for each use. On the contrary, as soon as music or video is played, even by means of digital equipments, there is an analog signal. What can be perceived by humans can also be captured and reproduced.

This phenomenon was called the "analog hole"[11]. For instance, even if a video is protected against copies, when somebody plays it on a computer or a VCR, nothing prevents him from capturing it by filming the screen with a digital camcorder in order to make several copies. It is the same problem for books that can be scanned, or music, that can be copied thanks to analog devices.

Thus, TPM on music and video was a thornier question than TPM on softwares. Companies like *Macrovision* have been trying since 1985 to prevent VCR to VCR copies by licensing to publishers a technology that exploits the automatic gain control feature[12] of VCRs. Similarly, since 2000, companies have been implementing copy protection schemes on CDs after the *Napster* scandal. However, this event has been the starting point of massive file-sharing practices. The most common system of protection made CDs unusable with computer's CD drives. The goal was to prevent the use of CD burner softwares that permitted the burning of CD copies from original CDs, or CD ripper softwares that enabled the conversion (or encoding) of audio CDs into digital audio files such as MP3.

Several other DRM systems have been created in the last years, and the impact of DRM also results in an evolution of regulation.

3. Evolution of regulation relative to DRM

[11] "*The term "analog hole" was first popularized by the Motion Picture Association of America and some of its members during speeches and legislative advocacy in 2002, this term later fell into disrepute within the industry, being replaced by analog reconversion problem, analog reconversion issue and similar terms*". http://en.wikipedia.org/wiki/Analog_hole

[12] c.f. technical glossary p.72

The first real debate relative to technology and copyright protection in Europe dates back to 1988, with the Commission's green paper on "copyright and the challenge of technology"[13]. Even if the Commission wanted copyright to be a stimulating instrument rather than a prohibitive one[14], a first proposal for a legal locking on technology to prevent digital copying was introduced: the possession of digital audio tape commercial duplicating equipment "*should be made dependent upon a licence to be delivered by a public authority and the maintenance of a register in respect of licensed equipment*"[15]. It probably inspired the United States ("US") Audio Home Recording Act of 1992 which required a serial copy management system in all digital audio recording devices ("DAT") allowing only first-generation copies[16].

But the decisive step came from the World Intellectual Property Organisation ("WIPO") copyright treaty adopted in Geneva on 20 December 1996[17]. Thus, Article 11 on Technological Measures clearly states: "*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*". And article 12(1) on Management information states: "*Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts* (...)*: (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*". The same obligations are provided for in article 18 and 19 of the WIPO Performances and phonograms treaty adopted the same day[18]. Beyond the mere protection of copyright facing technology, the WIPO introduced the protection of technology that protects copyright.

These treaties were implemented in the US by the Digital Copyright Millennium Act ("DCMA") of October 28th, 1998[19]. Section 1201 protects TPM against circumvention and Section 1202 protects the integrity of copyright management information. Infringements of

[13]COM/1988/0172 - Green Paper on copyright and the challenge of technology - Copyright issues requiring immediate action

[14] B. Posner, "Purposes and scope of the Green Paper on Copyright and the Challenge of Technology", in *Copyright and the European Community: The Green Paper on Copyright and the Challenge of New Technology* (F. Gotzen ed., 1989), p.2-8.

[15]COM/1988/0172; 3.13.1 (e) p.137 and Martin Kretschmer, "Digital copyright: the end of an era", *European Intellectual Property Review 2003*, 25(8), p. 335

[16] *The United States Code* Title 17 "Copyright Law of the United States of America and Related Laws" Chapter 10 "Digital Audio Recording Devices and Media" § 1002.
http://www.copyright.gov/title17/92chap10.html#1002

[17] WIPO copyright treaty, 20 December 1996 http://www.wipo.int/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf

[18] WIPO Performances and phonograms treaty, 20 December 1996
http://www.copyright.gov/wipo/treaty2.html

these provisions are punished on first offence with a fine of $500,000 or a five-year prison sentence.

Concerning the European Union ("EU"), a new Green Paper of July 27th, 1995 on "Copyright and related Rights in the Information Society"[20] stressed the need to develop technological systems of protection and identification in favour of rightholders. It engaged a consultation process which led to a new communication on Copyright and Related Rights on 20 November 1996[21] which stressed in particular the objectives of technical identification and protection schemes[22].

Finally, the ISD of 2001 was proposed and adopted in order to transpose the WIPO treaties, and articles 6 and 7 refer to WIPO's obligations relative to DRM protection. The ISD has now been implemented in most EU "historic" Member States.

In parallel, the EU has adopted the Directive on conditional access ("DCA") on 11 November 1998[23] which purpose is to prohibit devices that permit unauthorised access to services like Pay-TV, video-on-demand ("VOD") or electronic publishing. If there is no clear reference to DRM, nevertheless article 4 prohibits the manufacture, import, distribution etc. of circumventing devices, similarly to the provisions of article 6(2) of the ISD.

Finally, it must be noticed that softwares fall outside the scope of the ISD, and are covered by the "software directive" of May 14th, 1991[24]. However, article 7(1)(c) especially prohibits the act of putting into circulation or the possession for commercial purposes of "*any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program*". So the protection of DRM and especially TPM first appeared in the EU legislation with this article.

4. The context of information society

[19] The Digital Millennium Copyright Act (1998) http://thomas.loc.gov/cgi-bin/query/F?c105:6:./temp/~c105TjnYFD:e884:

[20] COM/1995/0382 - Green Paper - Copyright and Related Rights in the Information Society

[21] COM/1996/0568 – Commission communication -Follow-up to the Green paper on copyright and related rights in the information society

[22] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.288

[23] Directive 98/84 E.C. of the European Parliament and the Council on the legal protection of services based on, or consisting of, conditional access, *Official Journal* L320, November 11, 1998 p. 54-57

[24] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17.5.1991, p. 42–46

The ISD intends to combine the exigencies of copyright protection with the technological progress represented by the "information society". This expression describes a society in which information is the key element, and where the creation, distribution, diffusion and use of information constitute a basis for any economic, political or cultural activity[25].

This kind of society succeeds to the industrial society, given that the economic knowledge now relies on information, even related to industry, rather than industrial production in itself. The expression comes from research works that the economist Fritz Machlup realised in the thirties[26]. But of course, with the development of computers and massive networks since the late seventies, and in particular since the popularisation of Internet since the mid-nineties, this concept has evolved in a new light.

Nowadays, most activities are partially or completely established on the web, and information circulates the world over at high speed. So the notion of information society is now coupled with the one of "digital age", which implies that information on a digital form is easily transferable and reproducible, and so it is for copyrighted works.

Internet is not really regulated by law, and so copyright in the digital age raises serious issues, as soon as technology does not comply with law anymore[27]. Ironically (or pragmatically), DRM, which is mainly characterised by technological devices, tries to answer this technological breach: "*the answer to the machine is in the machine*"[28]. DRM encourages confidence, even if no rightholder believes in cent per cent effective technologies[29].

5. Current examples of DRM

[25] http://en.wikipedia.org/wiki/Information_society
[26] http://www.mises.org/content/aboutmachlup.asp
[27] Henning Wiese, "The justification of the copyright system in the digital age" *European Intellectual Property Review 2002*, 24 (8), p.387-396
[28] Charles Clark, "The answer to the machine is in the machine", *The Future of Copyright in a Digital Environment* (P. Bernt Hugenhotltz, ed., 1996), p. 139- 146.
[29] Florian Koempel "Digital Rights Management" *Computer and Telecommunications Law Review 2005*, 11(8), p.239

It is necessary to give a short outline of existing technologies that are currently used in the DRM perspective.

As far as TPM are concerned, most of them are anti-copy devices. Among them, the *Serial Copy Management Systems* (SCMS) has been often used on DVD videos, to prevent second-generation copies (copies can only be made from the original DVD). Similarly, the *Content Scramble System* (CSS) from *Matsushita Electric Industrial Co* and *Toshiba Corporation* is used to control access and reproduction of DVD movies. Access control systems use encryption devices.

Regarding music, the Secure Digital Music Initiative (SDMI) is a secured file format for music that is distributed online. It prevents unauthorised copying. But the most common format was the audio *Copy control* on CDs released by *EMI* and *Sony BMG Music Entertainment*. It prevented digital extraction by CD ripper softwares in order to curb file-sharing. Furthermore, DRM information restricted the use and copy with some operating systems, some softwares etc. However this format was mostly abandoned in 2006[30].

Concerning RMI, watermarking and fingerprinting, which are intended for identification and authentication of works and rightholders by means of hidden digital marks, are often used. These technologies enable tracing, and thus a long-term control of access and copy of works[31]. But RMI can also be mere identification standards, such as the International Standard Recording Code ("ISRC") which is an ISO standard used to identify sound recordings and music video recordings, or the International Standard musical Work Code ("ISWC") which is another ISO standard used to identify musical works, but not recordings[32].

[30] http://www.emimusic.info/us_EN/sect4.html

[31] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review* 1999, 21(6), p.286, and Patricia Akester, "Survey of technological measures for protection of copyright" *Entertainment Law Review 2001*, 12(1), p.37

[32] http://www.ifpi.org/content/section_resources/isrc.html and http://www.iswc.org/iswc/en/html/home.html

Other sadly notorious examples of DRM are the *Sony* rootkit and *Apple*'s protection devices which were important sources of discontent.

6. DRM and controversies

DRM and in particular TPM on softwares have always been a source of discontent, but it never reached the importance of the music DRM scandals.

In late 2005, *Sony BMG music* faced a scandal because of *Extended Copy Protection* ("*XCP*"), a TPM included on CDs of several artists. As soon as discs were inserted, the *XCP* software was installed in order to prevent the use of CD ripper softwares. Actually, *XCP* turned out to be a rootkit[33] that modified CD devices and drivers, and favoured the installation of malwares (virus, spywares, Trojan horses etc.) from outside. Indeed, such programs were hidden by the rootkit's digital cloak. After several lawsuits, *Sony BMG* eventually issued a product recall for the discs concerned and suspended the use of *XCP*[34]. Beyond the reputation of the firm, the reputation of DRM systems has been seriously harmed.

More recently, *Apple* has been accused of using "cripplewares" on *iPod* digital players. It was reproached to the firm to lock, to "cripple" *iPods*' interoperability[35] with other protected music formats like the ones of *Microsoft* (WMA DRM). Actually, the *FairPlay* (sic) copy protection device works as follows: consumers buy songs in *Apple*'s online music store *iTunes*. Songs can only be played by *iPod* players, which can only play protected music from the *iTunes* store (AAC DRM) or non-protected music (MP3). So, for instance, *Windows Media Player* cannot play *iTunes* music without circumvention. Similarly, an *iPod* cannot play *Sony*'s ATRAC music standard. It can only play *Apple*'s files and non-protected music files like MP3. The system is actually locked up[36].

The question of *Apple* devices' interoperability had a particular impact in France, with the implementation of the ISD by the law of August 1st, 2006[37]. The draft of the law already included an interoperability requirement for TPM that was considered to be a declaration of war to *Apple FairPlay* device. Indeed, it consisted in an obligation to give users "essential

[33] cf. Technical glossary p. 72

[34] Michael Geist "Legal fallout from Sony's CD woes" *BBC news* (3 January 2006) http://news.bbc.co.uk/2/hi/technology/4577536.stm

[35] cf. Technical glossary p. 72

[36] Randall Stross "Digital Domain: Want an iPhone? Beware the iHandcuffs" *New York Times* January 14, 2007 http://www.nytimes.com/2007/01/14/business/yourmoney/14digi.html?ex=1326430800&en=2c5efe51f9d74dd8&ei=5090

[37] Loi n° 2006-961 of 1 August 2006 "*relative au droit d'auteur et aux droits voisins dans la société de l'information*" *Official Journal* n° 178 of 3 August 2006, page 11529, called "DADVSI"

documentation" (TPM source codes) to ensure interoperability. *Apple* threatened to leave the French market and claimed that the law would hinder or even kill online music distribution. Eventually, article 14 of the final law created a new Regulatory Authority for Technical Measures ("ARMT") which mission is to assess the balance between work protection by DRM and lawful use, in particular as regards interoperability. This novelty softened a little *Apple*'s position given that the Authority can now play a role of mediator[38].

These examples are representative of the perception of DRM in our society. Whether they are a positive or a negative progress, contestations certainly fed distrust of users. It is unquestionable that DRM changed the copyright balance between the public interest and rightholders' interests.

7. The issue of DRM

Copyright law, as any intellectual property law, has to strike a balance between, on the one hand, the protection of works, and so the protection of rightholders, in order to create incentives for creation, and on the other hand, the protection of lawful users, of the public.

Rightholders are granted exclusivity and users are granted exceptions to this exclusivity. What is the place of DRM in this balance?

DRM systems are technical protections and identifications of works. In broad outline, they are on rightholders' side. Users have few exceptions or solutions against these devices. Indeed, they are protected by law against circumvention. So, users' exceptions to exclusive rights on copyrighted works are threatened by the spread of DRM.

Admittedly, DRM turns out to be harmful for users. Fair use is decreased and new consumptions patterns are looming. At the same time, fundamental freedoms such as freedom of expression or right to privacy are threatened, not counting the question of interoperability (Chapter II).

Nevertheless, even harmful, the creation of such a strong regime of protection for rightholders could be justified, if its actual necessity to ensure effective copyright protection in the information society was not so doubtful (Chapter I).

[38] Nicolas Jondet "La France v. Apple: who's the dadvsi in DRMs?" *SCRIPT-ed* (Volume 3, Issue 4, June 2006) p.7-8 http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/jondet.asp

Chapter 1. The creation of a strong regime of protection for rightholders whose necessity remains doubtful

The regime of DRM is particularly strong as the protection comes in three successive steps (Section A). It raises the question of the actual necessity of such a system in eventually protecting copyright (Section B).

Section A. "Electrifying the fence" [39]: the establishment of a three-steps regime of protection

With the ISD, works can be protected by a threefold system: works are protected by copyright, what is not new. The second step is more interesting, as the copyright protection is itself ensured by DRM (1). Finally, DRM is protected by anti-circumvention measures. This is the third step of protection (2)[40].

1. The protection of copyright by means of DRM

The protection of a legal protection (copyright) by technical means is a real novelty (b), whether it is done thanks to TPM or RMI (a).

a) TPM and RMI: two faces of the same coin

TPM and RMI, as previously defined, must not be opposed. Both are part of DRM, they are complementary, two faces of the same coin.

As article 6(3) of the ISD states, the notion of TPM refers to devices designed "*to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright or any right related to copyright"* Similarly, the notion of RMI

[39] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.285-297

[40] ibidem.

is defined in article 7(2), and refers to information provided by rightholders *"which identifies the work* (...)*, the author or any other rightholder, or* (...) *the terms and conditions of use of the work*".

The purpose of TPM and RMI is part of their definition. They are both designed to prevent any unauthorised act on protected works, by means of technical protections (TPM) and by means of identification of works and conditions of use (RMI). It consists in a double "wrapping", a digital protection shell, and a data ID card or explanatory leaflet for works.

b) Technical means to protect copyright

DRM protects the protection. It applies to protected works, whether they are protected by copyright or by related rights. The notion of "related rights" mainly concerns the *sui generis* right provided for in Chapter III of Directive 96/9/EC on databases[41]. Indeed, databases can be protected both by copyright if they are original, and by a special right when there "*has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*" (article 7(1) of the database directive).

So databases, as literary works, dramatic works, musical works, graphic works, cinematographic works etc. fall within the scope of DRM protection. And DRM protects works against unauthorised use, that is to say acts which are part of exclusive rights of authors (and other rightholders), as defined in Chapter II. It concerns the reproduction right (article 2), the right of communication and making available to the public (article 3), and the distribution right (article 4).

The reproduction right is of course the exclusive right to authorise or prohibit reproduction of works (or parts of them) in the broad meaning. Indeed, if it concerns works for authors, it also concerns fixations of performances for performers, phonograms and fixations of films for phonogram and film producers, and fixations of broadcasts for broadcasting organisations.

The notion of communication to the public generally consists in communicating a work to a present public, simultaneously, whereas the making available implies that the public will

[41] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077 , 27/03/1996 p. 20 - 28

access the work on a longer period of time. The first notion mainly refers to performing arts, but it can also concern TV or radio broadcasting. The notion of "making available" is more appropriate with Internet diffusions where communications are mostly indirect, on a long or perpetual period of time, and where the public is unknown[42].

The distribution right, or right to issue copies of the work to the public, has replaced the former publication or divulgation right and consists in a right of first sale, which is exhausted as soon as it is performed[43].

Therefore, these rights are ensured by DRM systems. On one side, TPM restrict access and reproduction possibilities of works to prevent unauthorised copying, communication, making available or distribution. On the other side, RMI enables identification of works. It can trace them to prevent unauthorised acts. But it also exposes the terms and conditions under which the rightholder wants works to be used, copied or made available. Thus, it may as well protect any licence granted on works concerned. A licensee could be registered in the metadata[44] of a work and so have particular rights on it. Rights are identifiable by any user according to RMI systems[45].

The final goal of such measures is to fight against "piracy", in particular on the web, by means of tracing and locking devices on works. The identification of works, rightholders and conditions of use can also enable identification of users and debtors. TPM prevent unlawful acts, and the spread of unlawful copies. At that point we may also think that TPM can protect RMI against removal, as soon as they lock up all components of works.

2. The protection of DRM against circumvention practices

The legal protection of DRM, which is a technical protection, characterises the notion of "*electrifying the fence*" highlighted by Dr Severine Dusollier (University of Namur). The system is strengthened, locked up[46]. To try to disable the technical protection is punished with an "electrical discharge": anti-circumvention provisions (a). This punishment may be similar to the one relative to copyright infringements (b).

[42] L. Bently and B. Sherman, *Intellectual Property Law* (Oxford University Press 2nd edition 2004) p.143-145
[43] ibidem. p.137
[44] cf. Technical glossary p.72
[45] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.295
[46] ibidem.

a) Legal measures to protect technical protections

It is necessary to distinguish the protection of TPM (i) and the protection of RMI (ii), as the scope of protection is not the same.

i. The protection of TPM against circumvention

Article 6 (1) of the ISD states "*Member States shall provide adequate legal protection against the circumvention of any effective technological measures which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective*". The protection of article 6 covers certain devices (1), against certain acts (2), but may tolerate some exceptions (3).

1) A wide object of protection

First, the exact object of the protection must be assessed. The ISD gives legal protection to "*any effective technological measures*" (article 6(1)). Article 6(3) gives two criteria of definition: a criterion of purpose and a qualitative criterion[47].

The criterion of purpose states that protection is only given to TPM which "*are designed to prevent or restrict acts* (...) *which are not authorised by the rightholder of any copyright* (...)" or any *sui generis* right on a database, as already evoked. So, on the contrary, the ISD does not protect TPM designed to prevent any other act, like for example unauthorised access to patent information, undisclosed information or trade secrets, or access to works already fallen within the public domain.

The criterion of efficiency states that protection is only given to TPM which are "effective", that is to say "*where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective*". (article 6(3)). Thus, TPM are effective when they are "*the lock and the bolt on copyright's door*"[48].

[47] Michel Vivant, Lucien Rapp, Michel Guibal, Bertrand Warusfel, Jean-Louis Bilon and Gilles Vercken, *Lamy Droit de l'informatique et des réseaux* (Lamy 2004) n° 2580

[48] Translated from a French quotation in Christophe Caron, *Droit d'auteur et droits voisins* (Litec 1st edition 2006) p.261

Anyway, the criterion of efficiency is quite hard to assess. Indeed, we may affirm that all TPM are likely to be "cracked", circumvented. So no one is absolutely effective.

But, on the other hand, according to the definition given by the ISD, as soon as TPM create an "*access control or protection process*", they can be considered "effective", even if the protection is eventually circumvented and so is inefficient. So, according to article 6(3), the ISD protects both access control TPM and copy control TPM, even if the DCMA is clearer on this point[49].

Nevertheless, effectiveness remains a matter of willingness for rightholders. Obviously, they would not use TPM if they did not think them effective, at least for their deterrent effect. They always believe in their effectiveness and TPM always control access, or apply protection processes. So every TPM is likely to be protected.

To go further, if TPM were actually effective, why would they need legal protection against circumvention? The question must be raised, given that the Helsinki District Court recently released a unanimous decision (on 25 may 2007) where it ruled that CSS used in DVD movies was not effective as defined by law. The Court stated that CSS no longer achieved its protection objective as end-users could get circumventing softwares from the Internet, even free of charge (since the young Norwegian Jon Lech Johansen cracked the protection in 1999)[50].

Therefore, this criterion is very unclear, anyway, it could make the scope of protection very wide.

[49] Terese Foged, "US v EU anti-circumvention legislation: preserving the public's privileges in the digital age", *European Intellectual Property Review 2002*, 24(11), p.537

[50]Ketola (Afterdawn) "CSS protection used in DVDs "ineffective" Finnish court rules" (25 May 2007) http://www.afterdawn.com/news/archive/9849.cfm and Helsinki District Court Judgment 07/4535 - 4/10 Dept. 25 May 2007 R 07/1004 http://www.turre.com/css_helsinki_district_court.pdf

2) The scope of prohibited acts

Concerning acts prohibited, article 6(1) implies that the circumvention of TPM is prohibited, as soon as the persons concerned "*carr*[y] *out in the knowledge"* or have *"reasonable grounds to know"* that they are actually circumventing TPM.

The knowledge of circumvention purposes is linked with the second step of prohibition which covers, beyond the mere circumvention, "*the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of 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 TPM (article 6(2)).

So it concerns preparatory activities to circumvention: commercial trafficking in TPM circumventing devices or the provision of services for TPM circumvention purposes. It refers to the notion of secondary infringement in Anglo-Saxon copyright law: to provide accessories used to infringe rightholders' exclusive rights or to assist in the making or distribution of infringing copies[51].

Moreover, article 6(2)(b) and especially 6(2)(c) refer to the "*Betamax Defence*", from the eponymous case relative to *Sony*'s video recorders (*Betamax*) in which the US Supreme Court held that "*a technology vendor could not be held liable for distributing a technology capable of substantial non-infringing uses"*[52]. As regards TPM, the provision of services, or trafficking in devices that can enable the circumvention of TPM, but that are also capable of substantial non-circumventing uses, is not prohibited.

The problem is, as usual, to define what is substantial, and what is not, and precisely what is a "*limited commercially significant purpose or use*" (article 6(2)(b)) and what means "*primarily designed*..." (Article 6(2)(c)) as regards proportion[53].

[51] Copyright, Designs and Patents Act ("CDPA")1988 (C.48), s. 26
[52] *Sony Corp. of America v. Universal Studios Inc.*, 464 U.S. 417 (1984)
[53] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.296

The recent case *Sony Computer Entertainment v. David Ball*[54] highlighted this problem, even if it dealt with softwares, which are outside the scope of the ISD. The defendant, David Ball, designed, sold, manufactured and installed chips to be inserted into *Sony*'s *PlayStation2* in order to enable players to circumvent the copy protection devices (With the chip, the console believed that mere copies were original DVDs). He tried to argue in particular that his device did not have the "*sole intended purpose*"[55] of facilitating the unauthorised circumvention of the technical device (the copy protection), but also has a legitimate purpose: to make back-up copies. The Court eventually held that *Sony*'s storage devices (DVDs) were robust enough, and that even if they were damaged, *Sony* agreed to replace them. So, back-up copies were useless and no legitimate purpose could be argued for the use of the chips[56].

Even if the "*betamax* defence" had maybe a wider scope in this case than the one of the ISD (because "*sole intended purpose*" is stricter than "*primarily designed*"), it did not succeed.

3) Exceptions

Finally, the protection of TPM tolerates exceptions given that article 6(4) compels Member States to take appropriate measures to ensure that rightholders make available to the beneficiary of exceptions provided for by national law, in accordance with provisions of article 5 of the ISD (such as research, educational exceptions etc.), the means of benefiting from them to the extent that this beneficiary has legal access to the protected work.

Nevertheless, the provisions of article 5 are not compulsory, except the one of article 5(1) relative to temporary acts of reproduction "*which are transient or incidental [and] an integral and essential part of a technological process* (...)". It refers to reproduction acts that are necessary to enable a lawful use of a work, especially in a digital environment (cookies[57], temporary files, cache files etc.). The other exceptions are optional provisions that Member States can implement or not.

Anyway, all exceptions must fulfil the Berne three-step test[58] according to article 5(5) which provides that: "*The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of*

[54] *Sony Computer Entertainment UK Ltd v Gaynor David Ball & 6 Ors* [2004] EWHC 1738 (Ch)

[55] The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003 (amending the CDPA of 1988) s.296(1)(b)(i)

[56] Helen Padley, "Copyright – games – copy circumvention device (case comment)" *Entertainment Law Review 2005*, 16(1), N9 and Michael Flint, Nick Fitzpatrick and Clive Thorne, op.cit. p.469

[57] cf technical glossary p.72

[58] Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, revised at Paris on July 24, 1971, and amended on September 28, 1979, article 9(2)

the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

ii. The protection of RMI against removal

If TPM are "*the lock and the bolt on copyright's door*", RMI is the "*number plate of works*"[59]. And as for TPM, RMI systems are protected against circumvention, or more properly against removal. Thus article 7(1) of the ISD prohibits (a) the act of knowingly removing or altering any electronic RMI without authority and (b) "*the distribution, importation for distribution, broadcasting, communication or making available to the public of works* (...) *from which electronic rights-management information has been removed or altered without authority*" as soon as the person "*knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright* (...)".

As for the protection of TPM, the protection of RMI only concerns information that identifies works protected by copyright, databases protected by the *sui generis* right, or any information or codes about the terms and conditions of use of these works or databases (article 7(2)).

Moreover, the removal of RMI is forbidden just like the trafficking of works from which RMI has been removed or altered. Quite surprisingly, there is no analogy with article 6(2), which prohibits preparatory activities. Indeed, Article 7 could have prohibited the manufacture, import etc. of products or components, or the provision of services which enabled the removal or alteration of RMI without authority, when the devices or services had only a limited commercially significant purpose or use other than removal or alteration, or when they were primarily designed for the purpose of enabling or facilitating the removal or alteration of RMI.

[59] Translated from the French quotation in Christophe Caron, *Droit d'auteur et droits voisins* (Litec 1st edition 2006) p.261

As it is not the case, the protection of RMI strictly concerns removal and trafficking of altered works, what seems narrower in appearance. But on the other hand, the trafficking of works where TPM have previously been circumvented does not constitute a prohibited act in itself.

Furthermore, contrary to TPM, the protection of RMI does not ensure users' exceptions to copyright. However, it may present fewer problems given that RMI is not supposed to curb these exceptions.

b) Is DRM circumvention copyright infringement ?

The ISD states that the circumvention of DRM, whether it is the circumvention of TPM or the removal of RMI, shall be prohibited, although article 6 is not perfectly clear on this point.

Indeed, it provides that Member States must ensure legal protection against circumvention that the person concerned commits, but it eventually does not clearly state that the act of circumvention is prohibited in itself and consequently punished. Actually, article 6 only provides for positive obligations for states to prevent circumvention, preparatory activities and trafficking in devices.

Similarly, article 7 provides that Member States must ensure legal protection against removal and trafficking without clearly stating that the act of removal must be punished.

Article 8 is not a great help to us as it only states: "*Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in*

this Directive…". It clearly refers to copyright infringements relative to rightholders' exclusive rights provided for in article 2, 3 and 4. Besides, contrary to these three articles, none of article 6 and 7 utilises the term "prohibition".

So, nothing in the ISD enables us to say how DRM circumvention is punished, and to what extent it could be considered copyright infringement[60]. This question is important because even if circumvention can lead to copyright infringement, it can also be justified by interoperability purposes without any infringement purposes[61].

The writing of article 6 and 7 of the ISD could remind criminal provisions, such as those relative to repression of computer fraud. In such a case, circumvention would not be considered copyright infringement. Besides, most European countries have implemented the directive in this way, and consider that the circumvention of DRM constitutes a criminal offence or a civil tort (when it is exclusively done for private use)[62].

It is also the case for the United Kingdom ("UK"), which implemented the ISD in October 2003 by the Copyright and related rights regulations[63] amending the CDPA of 1988.

In the UK, the circumvention of TPM in itself is now punished by means of civil remedies, and never with criminal penalties (CDPA, s.296ZA.). But trafficking in devices enabling circumvention constitutes a criminal offence punished with a fine and/or a prison term of up to two years (CDPA, s.296ZB). Similarly, the removal or alteration of RMI does not constitute a criminal offence but involves civil liability (CDPA, 296ZG)[64].

Concerning France, the ISD has been implemented by the law of August 1st, 2006[65] ("DADVSI"). Now, the circumvention of TPM constitutes a criminal offence according to article L.335-3-1 of the Intellectual Property Code ("CPI"), as well as the removal or alteration of RMI (L.335-3-2 CPI). The mere circumvention (of effective TPM) or removal is punished with a fine of 3750 euros. Trafficking in devices enabling circumvention, or incentives for use of such devices is punished with a fine of 30 000 euros and a prison term of six months (L.335-3-1-II CPI). The same punishment is provided for the trafficking of

---

[60] Kamiel J. Koelman, "A hard nut to crack: the protection of technological measures", European *Intellectual Property Review 2000*, 22(6), p.279

[61] Mikko Valimaki and Ville Oksanen "DRM interoperability and Intellectual Property policy in Europe"

European Intellectual Property Review 2006, 28(11), p.562-568

[62] Isabelle Vaillant "Le contournement des mesures techniques de protection, contrefaçon ou criminalité informatique ?" (June 2003) p.13-15 http://eucd.info/documents/transposition-eucd-2003-06-20.pdf

[63] The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003

[64] Michael Hart and Steve Holmes "Implementation of the copyright directive in the United Kingdom" *European Intellectual Property Review 2004*, 26(6), p.254-257

[65] Loi n° 2006-961 of 1 August 2006 "*relative au droit d'auteur et aux droits voisins dans la société de l'information" Official Journal* n° 178 of 3 August 2006, p. 11529, called "DADVSI"

works where RMI has been removed or altered in order to undermine copyright (L.335-3-2-III CPI). Surprisingly, the law goes beyond the directive because the same punishment is also provided for trafficking in devices enabling the removal or alteration of RMI in order to undermine copyright, or incentives for use of such devices (L.335-3-2-II CPI).

Anyway, none of these national laws seem to consider that DRM circumventions (or removals) constitute copyright infringement. Indeed, DRM systems are not part of rightholders' exclusive rights, they only protect them. And only infringement of exclusive rights is considered copyright infringement[66]. So the question is raised: was it necessary to protect DRM in parallel with copyright protection?

Section B. Is the answer to the machine in the machine?[67]: the doubtful necessity of technology to protect copyright

The need to protect copyright by technical means appeared in the context of the information society (1), however, the question of the role of technology in copyright law remains particularly tricky, even in that context (2).

[66] Christophe Caron, "Brèves observations sur la protection des mesures techniques par le droit civil" *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/pres_caron.doc

[67] Charles Clark, "The answer to the machine is in the machine", *The Future of Copyright in a Digital Environment* (P. Bernt Hugenhotltz, ed., 1996), p. 139- 146

1. The attempt of justification by the need for protection in the information society

The information society and in particular the digital age brought new issues for copyright (a), but nothing proves that DRM is an appropriate answer to these new problems (b).

a) An unquestionable evolution towards a digital society

The evolution towards the digital age, as already evoked, inspired the WIPO treaties of 1996 and so the ISD. Even if 1996 was the prehistory of this phenomenon, the WIPO already foresaw the problems the digital environment would raise for copyright.

Indeed, facing the Internet and new technologies, copyrighted works (and related works) are more vulnerable given that digital copies are perfect, loss less, and can be shared with the whole world instantaneously[68]. On the web, anybody can get copyrighted works from any part of the world in a couple of minutes, in particular thanks to file-sharing systems such as *KaZaA, Emule, Grokster* etc. and networks like *BitTorrent, Gnutella* etc.. They are often called "peer-to-peer" systems because they imply file-uploading and file-downloading from user to user, without any central server, contrary to the old *Napster*. Since the first shutdown of their common ancestor, they have spread, and now, there are millions of users[69].

As there is no central server, it is very hard to make these systems shut down. However, it may have a strong economic impact for rightholders and the entertainment industry. Therefore, rightholders have looked for a technical answer to this problem. Indeed, a lack of copyright protection may involve a lack of incentives for creation, and may as well undermine business models[70].

But perhaps the apparent loss of control in the digital environment is just a transitional period which reveals early fears, as the spread of VCR did in the early eighties. Perhaps copyright owners could overcome the digital age and eventually benefit from it. And maybe

---

[68] Nora Braun, "The interface between the protection of technological measures and the exercise of exceptions to copyright and related rights: comparing the situation in the United States and the European community" *European Intellectual Property Review 2003*, 25(11), p.503

[69] BPI *Online Music &UK Record Industry* p.3, http://www.bpi.co.uk/pdf/Illegal_Filesharing_Factsheet.pdf

[70] Barry B. Sookman "Technological protection measures (TPMS) and copyright protection: the case for TPMS" *Computer and Telecommunications Law Review 2005*, 11(5), p.147

it would have been wiser to wait and see the evolution, before strongly protecting copyright by DRM, and DRM by law[71].

b) The acknowledgement of DRM's inefficiency in regulating this evolution

The mere evolution of society is not sufficient to justify the need for DRM, it is also necessary to prove that DRM can counter "piracy" (i) and in particular the one that undermines music industry (ii).

[71] Kamiel J. Koelman, "A hard nut to crack: the protection of technological measures", European *Intellectual Property Review 2000*, 22(6), p.279-280

i. The relative inefficiency in fighting against "piracy"

DRM is mainly designed to cope with "piracy" that is to say copyright infringements. However, the technological race between TPM creators and crackers turns out to be desperate given that publishers are bound by commercial exigencies when they use new TPM. For example, the Content Scramble System (CSS), which is used on DVDs, is a copy protection system using very strong encryption methods. It has been broken since a long time (1999). Nevertheless, this standard of encryption cannot be changed because it would render all DVD players sold prior to this change unusable with new DVDs. It would be a commercial disaster[72]. So they must accept this situation. Similarly, common TPM such as *Macrovision*, *SCMS* or *SDMI* have already been circumvented. So, DRM's usefulness is short.

Crackers use reverse engineering[73], what is a set of technical methods that permit to understand how softwares work. So, beyond scientific fair use, it can enable the unlocking of softwares, and TPM circumvention[74]. But this method also has significant scientific usefulness. The main problem is that, as soon as a breach has been found in a DRM system, it can be incorporated in a software, and spread, so as any amateur can easily circumvent the protection[75]. It is very quick. Actually, for some crackers, DRM even constitutes a challenge, it stimulates them. For some others, it can have a deterrent effect, until someone finds a breach and discloses it.

One solution could be "trusted computing" where a content player only send digital output to a "trusted" output device. Users do not have access to the platform, to the software, they just access the content what limits the possibilities of reverse engineering[76]. Nevertheless, restricted access raises numerous issues relative to fair use.

Therefore, DRM, which is mainly designed to fight against copyright piracy, is itself victim of piracy, of circumvention.

Moreover, as already evoked, even if DRM is not broken, the "analog hole" problem remains. It is not always necessary to circumvent DRM in order to make copyright infringements, it can be easier to burn a CD with DRM-protected music and then to encode it in MP3, or to record files played on a computer by means of analog devices such as

---

[72] Tony Smith "Tiny C code bests seven-line DVD decoder" *The Register* (13 March 2001) http://www.theregister.co.uk/2001/03/13/tiny_c_code_bests_sevenline/

[73] cf technical glossary p.72

[74] Tomasz Rychlicki "An opinion on legal regulations on reverse engineering and technological protections measures" *Computer and Telecommunications Law Review 2007*, 13(3), p.94

[75] Barry B. Sookman, op. cit. p.146

[76] Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.165

recorders or camcorders. It is easy then to re-digitise or re-encode the works, even if quality is a little lower[77].

Thus, piracy must be taken into account by rightholders as an inevitable factor that is part of their economy. Current DRM could only have a residual deterrent effect on users. But the problem will also be not to let DRM costs outweigh its benefits[78]. As expressed by Shapiro and Varian: "*We think the natural tendency is for producers to worry too much about 'protecting' their intellectual property. The important thing is to 'maximize the value' of your intellectual property, not to protect it for the sake of protection. If you lose a little of your property when you sell it or rent it, that's just a cost of doing business, along with depreciation, inventory losses, and obsolescence*.[79]"

ii. The inefficiency of DRM in ensuring the music industry's health

According to more and more music labels and online services firms, DRM is not working. It is time to switch to unprotected formats[80]. Indeed, online music incomes do not compensate for the CD crisis according to the IFPI's digital music report 2007[81], and so new business models such as unprotected music selling or legal file-sharing must be explored[82].

The best example is the success of online stores without DRM such as *eMusic*. The store only sells MP3-encoded music (without protection). It was launched in Europe in 2006, and

[77] Ibidem. p.164-165
[78] Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan op. cit. p.9
[79] C. Shapiro and H. Varian, *Information Rules: A strategic guide to the network economy* (Harvard Business School Press, Boston 1999) p.97
[80] Adam Webb "It's the last rites for DRM…" *Music Week* (10 February 2007) p.9
[81] International Federation of the Phonographic Industry (IFPI) *Digital Music Report* (January 2007) p.4 http://www.ifpi.org/content/library/digital-music-report-2007.pdf
[82] Adam Webb op. cit. p.10

after two months, it had 20 000 subscribers and had sold about two millions tracks. It is now the number-two service in Europe.

But as *Jupiter Research* (online services for businesses) Vice President Mark Mulligan explained, it is not only a technical or economical question, but also a psychological one: "MP3" and "peer-to-peer" remain emotive words for the music industry and have connotations of "*online anarchy and rampant piracy*". "*MP3 was killing the business, and so for the majors* [it] *would be a huge psychological step. It would also be an irreversible step*"[83].

Anyway, this idea gained ground given that Steve Jobs himself (CEO of *Apple inc*.) thought about it. In a public letter of February 6, 2007[84], he contemplated three possibilities for the future of music industry and DRM. The first one was to continue on the current course: to keep the current system where the market is divided between different competitors (mainly *Sony*, *Apple* and *Microsoft*) which have their own proprietary DRM format, without any possibility of interaction between them. The second alternative was to license future competitors to develop these proprietary DRM standards, in order to ensure interoperability between music stores. Finally, the third alternative was simply to abolish DRM systems entirely.

Steve Jobs confessed that the third one was "*clearly the best alternative for consumers, and Apple would embrace it in a heartbeat*". He admitted that DRM systems were quite useless to fight against piracy and even harmful for the music industry as soon as, in 2006, 2 billion DRM-protected songs were sold worldwide by online stores while over 20 billion songs were sold DRM-free or on unprotected CDs[85].

Even if it is perhaps a question of consumer habits, it seems obvious that DRM-free music is more attractive for consumers. *Apple*'s CEO concluded that music companies had to choose the third alternative so that *Apple* might sell DRM-free music with their consent. Indeed, *Apple* recently began to sell DRM-free music files on *iTunes*. Actually, *Apple* just sells TPM-free files with very strong RMI systems, and they are 30% more expensive than TPM protected files[86].

Anyway, the main economic justification of DRM is about to collapse: DRM is not a good thing for the music industry. So, if it is unnecessary, the place of DRM provisions in a copyright directive becomes really doubtful.

---

[83] ibidem.

[84] Steve Jobs "Thoughts about music" (February 6, 2007) http://www.apple.com/hotnews/thoughtsonmusic/

[85] ibidem.

[86] Christophe Gauthier "Sans DRM, mais pas sans restrictions" *L'ordinateur individuel* (n°196 July-August 2007 p.14)

2. The tricky issue of the role of technology in copyright law

Facing the doubtful usefulness of DRM, the question to be raised is the following: is the answer to the machine in the machine, and does copyright law really need technology (a)? Maybe better solutions than anti-circumvention measures (b) or even DRM (c) could have been found to ensure copyright protection.

a) To what extent does copyright law need technology?

Law sometimes resorts to technology as a mean of enforcement. Technical databases or tracing methods are often used to enforce criminal law. Digital marking such as watermarking or fingerprinting, access restriction and cryptology[87] are used in several areas, from national security to trade secret. Moreover, competition law or civil torts in themselves cannot guarantee that traders do a completely fair business. As far as copyright law is concerned, DRM combines different methods such as identification (and tracing), content protection and cryptology.

In the digital age, as laws dealing with the Internet are considered to be already out of date before coming into force, only technology could be an adequate answer[88]. Thus, we made the first move towards *Lex informatica*, a new pattern where the Internet would be auto-regulated by technology, and where technologists would set new rules[89]. Such a system would certainly be faster, cheaper and fully enforced. However, it would definitely dismiss copyright law, and probably not in favour of users.

On the other hand, as already evoked, copyright law outlived the apparition of libraries in the XIX century and the apparition of the VCR in the early eighties, so why not the digital era? The true question is: does copyright need technology to outlive a technological threat? We might argue that DRM inefficiency has almost be proved, and so there is no need for technology in copyright law. However, Henning Wiese (Lawyer – Ministry of Justice of Lower Saxony) explains that we need both technology and anti-circumvention provisions by means of the "Information Superhighway" metaphor: "*Who would seriously question the need for traffic regulation per se just because it is technically possible to ignore a red light or a roadblock which are provided as technological measures to protect the health of other road users? Not all offenders will be caught; that will always be impossible in practice. However, the combination of both technology and law provides for two important and effective functions: infringement prevention (technology and law) and infringement repression (law). These functions do not prevent all infringements, but they make life on the "Highway" much safer.*"[90]

Once again, as we talk about DRM' usefulness, we refer to the deterrent effect of this technology: the difficulty to circumvent it and the fear of repression. As Henning Wiese himself concludes, we above all need a sound copyright law that creates strong incentives for creation and strong disincentive for hackers[91].

[87] Cf technical glossary p.72
[88] Henning Wiese, op. cit p. 388
[89] Joel R. Reidenberg " Lex Informatica: The Formulation of Information Policy Rules Through Technology" *Texas Law Review* (Volume 76, Number 3, February 1998) p. 566, Table 1C http://reidenberg.home.sprynet.com/lex_informatica.pdf
[90] Henning Wiese, op. cit p. 394
[91] Ibidem. p.395

Nevertheless, it raises serious questions in practice. Even if we recognised potential usefulness in DRM and in anti-circumvention provisions, it would remain tricky to argue that these provisions have anything to do with copyright law. Copyright protects authors' monopoly, rightholders' exclusive rights[92]. Anti-circumvention provisions do not directly protect these rights. Furthermore, DRM can also protect files that are not copyrighted works or databases. Then, they fall outside the scope of the ISD. Therefore, could there be any alternative to this pattern?

b) Alternatives to anti-circumvention provisions provided for in the ISD

Several solutions could have been found to protect DRM, rather than a copyright directive.

[92] Christophe Caron, "Brèves observations sur la protection des mesures techniques par le droit civil" *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/pres_caron.doc

i. The conditional access directive alternative

The European Community ("EC") directive of 1998 on Conditional Access[93] could have been more appropriate than the ISD to protect DRM, and in particular TPM, against circumvention.

Indeed, according to article 1 of the Conditional Access Directive (the "CAD") the objective of the text is to approximate provisions in Member States concerning measures against illicit devices which give unauthorised access to protected services. Article 4 prohibits trafficking in such devices very similarly to article 6(2) of the ISD. The services concerned are mainly pay-tv, video-on-demand and electronic publishing. Even if recital 21 of the CAD and recital 60 of the ISD provide that the directives are without prejudice to the application of each other, they may overlap in practice.

Indeed, the main difference between the protection of the CAD and the one of the ISD is that the latter protects access to works or other subject matters whereas the CAD protects access to services. But in the case of an online access to a database, the service is the protected matter, and so the two directives overlap[94].

[93] Directive 98/84 E.C. of the European Parliament and the Council on the legal protection of services based on, or consisting of, conditional access, *Official Journal* L320, November 11, 1998 p. 54-57

[94] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.290

Admittedly, the CAD protects *de facto* the remuneration of service providers and not authors' rights. But the remuneration of service providers includes royalties for copyrighted works broadcasting. Moreover, service providers are often rightholders, or directly linked with them. For example, *Apple iTunes*' DRM system is covered by the ISD, however *Apple* is not the rightholder of the works concerned. It is just the service provider: it sells music on behalf of rightholders. Nevertheless, the DRM system indirectly protects *Apple*'s service because if rightholders' works are not protected, the service disappears. So what is the difference between *Apple iTunes* and *Sky TV*'s pay-tv, which is a conditional access service that broadcasts copyrighted movies? The main difference is probably that *Apple*'s DRM does not only protect access to the service, but also digital reproduction of works obtained thanks to the service. However, as soon as DRM is used to control access to services linked with copyrighted works or databases, both directives cover it[95].

Therefore, the CAD protection could have been extended to any DRM system, whether it actually protected a work or a mere service.

[95] ibidem. p. 294

ii. The software directive alternative

Some DRM systems (and especially TPM) could be protected by the software directive of 1991[96], as soon as they are computer programs, and given that this directive protects by copyright "*the expression in any form of a computer program*" (article 1(2)). It must be original, that is to say, it must be the author's own intellectual creation (article 1(3)). According to article 7, Member States must prohibit trafficking or possession for commercial purposes of infringing copies of softwares, as well as "*any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program*" (article 7(1)(c)).

If we protected TPM like softwares, rightholders would be able to restrict the reproduction, the adaptation, the alteration or the distribution of his protection system (article 4). Besides, acts of circumvention often include a reproduction, an adaptation, and especially an alteration of a program. Authors would also be protected against decompilation[97] performed for purposes other than the need for interoperability (article 6).

Nevertheless, the main problem is the following: to prohibit under article 4 the infringement of TPM softwares that protect copyrighted works, the rightholder of these works should also be the rightholder of the softwares[98]. So, this protection is not really adapted to DRM.

iii. Other alternatives

Finally, several other legal protections for DRM could be contemplated, such as civil rules or simply criminal law.

Concerning civil rules, trafficking in circumvention devices may be harmful for rightholders, what involves liability of the persons who committed the acts. These persons will have to pay damages to rightholders. The problem is the burden of proof, because rightholders will have to prove harm, such as unfair competition harm. Eventually, they will probably have to prove that the manufacturing and selling of such devices effectively enable copyright infringement. However it is often merely hypothetical, except when the "*sole intended purpose*"[99] of the devices is to enable circumvention[100].

[96] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17.5.1991, p. 42–46
[97] cf technical glossary p.72
[98] Severine Dusollier, op.cit. p. 286
[99] The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003 (amending the CDPA of 1988) s.296(1)(b)(i)
[100] Severine Dusollier, op.cit. p. 287

Regarding criminal law, computer crime regulations already prohibit unauthorised access to some protected services, files or servers in most countries[101]. But computer crime could as well prohibit unauthorised access to non-free services, whether they are based on copyrighted works or not. Similarly, it could prohibit the manufacturing, advertising, selling etc. of circumvention devices that allow such unauthorised access, or any removal or alteration of technological information or identification attached to the contents.

The punishment would have to be proportionate to the level of knowledge, and the beneficiaries of the protection would be the service provider, the rightholders of the DRM system, and the rightholders of the copyrighted works that are accessible. Anyway, adequate exceptions for lawful users and for interoperability purposes would have to be granted[102].

c) Alternatives to DRM systems

Several alternatives could also have been found to protect copyright rather than DRM and its protection by the ISD.

[101] e.g articles 323-1 to 323-7 of the French criminal code or s. 1 to s.3 of the Computer Misuse Act 1990 (c. 18)
[102] Severine Dusollier, op. cit. p. 295

i. The Intellectual Property Rights enforcement Directive

The directive on enforcement of Intellectual Property Rights of 2004[103] could be regarded as an alternative to DRM systems. Its purpose is to enforce Intellectual property rights through a reinforcement of measures, procedures and remedies in this area (article 1).

Rules relative to the burden of proof are lightened in favour of rightholders (article 6). Moreover, Member States must ensure that before the commencement of any proceeding, judicial authorities will be able to take measures such as taking samples, or seizing goods without the other party having been heard, when there is reasonable evidence of infringements, and under several conditions (article 7).

Furthermore, according to article 8, the claimant in the context of proceedings concerning infringements can obtain information about the origin and distribution networks of the infringing goods or services (such as names, addresses, quantities etc.).

[103] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights *Official Journal* L 157, 30.4.2004, p. 45–86

Articles 6 and 8 only concern infringements carried out on a commercial scale (recital 14). Anyway, this kind of provisions may certainly have a strong impact on the protection of copyright against infringement, what is also the aim of DRM.

Nevertheless, this directive only deals with proceedings whereas DRM enables an *ex ante* control, before the committing of infringements, as soon as works are disclosed.

ii. Levies in favour of rightholders

The system of copyright levies has been created to compensate for the infeasibility of copyright licensing and enforcement. It normally consists in imposing a remuneration paid by manufacturers, importers and distributors of devices enabling reproduction, such as recorders, blank media, but also hard disks etc. If it unofficially compensates for potential

copyright infringements, it is normally designed to compensate for lawful exceptions to authors' exclusive rights.

If levies primarily rely on manufacturers and importers, they nevertheless pass the charge on consumers by means of reproduction equipments selling. The system is quite similar to the V.A.T one, and several European countries have implemented their own system to compensate for the private right to copy[104]. The UK is not concerned, as this exception does not exist.

Admittedly, DRM could now replace levies, as soon as it is supposed to ensure copyright licensing and enforcement[105].

[104] for a short framework of the French system :
http://www.sppf.com/en/protectionDroits.php?PHPSESSID=54ed0e39effae6a2c653576dbb6e14df
[105] Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.159-160

However, to have a claim to fully replace levies, DRM should correspond to an element of the Berne three-step test[106], also stated by article 5(5) of the ISD. Indeed, levies correspond to the third step of this test, the need not to "*unreasonably prejudice the legitimate interests of the rightholder*", and so, the need to give rightholders a fair compensation. It is particularly important to compensate for the private copying exception of article 5(2)(b). Besides, the fair compensation is also stated in article 5(2)(a).

[106] Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, revised at Paris on July 24, 1971, and amended on September 28, 1979, article 9(2).

In the ISD, DRM is regarded as being part of the three-step test, given that its purpose is to curb exceptions or infringements which "*unreasonably prejudice the legitimate interests of the rightholder*". It is part of "fair compensation".

Moreover, it is also indirectly part of this test as DRM and levies co-exist and are interdependent. Indeed, according to recital 35, "(...) *the level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive. In certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise*". So levies are likely to be reduced according to the

strength or spread of TPM, to avoid systems to be redundant. But on the contrary, could it be possible to lighten the level of TPM by spreading or increasing levies?

According to Dr Patricia Akester (University of Cambridge)[107], levies will disappear because of DRM's efficiency. So levies may not constitute an adequate alternative to this technology.

However, after having proved the relative inefficiency of DRM, despite its strong system of protection by law, we may also highlight its harmful consequences for users. It could eventually make people prefer levies to DRM. Indeed, according to the European Commission: "*Arguably, the widespread deployment of DRMs as a mode of fair compensation may eventually render existing remuneration schemes (such as levies to compensate for private copies) redundant, thereby justifying their phasing down or even out. At the same time, in their present status of implementation, 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 rightholders or those of legitimate users, consumers and other third parties involved* (...)"[108].

[107] Patricia Akester, op. cit. p.165

[108] COM/2004/0261 final - 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, 1.2.5, p. 10

Chapter 2. The harmful implications of DRM for users: revising consumption of works downwards

DRM has obvious impacts on the copyright balance and on fair use (Section A), but it also has more insidious impacts on fundamental rights that concern all users (Section B).

Section A. DRM's blindness[109]: the unfavourable evolution of fair use

Above all, it is necessary to define the notion of "fair use", as it is not really a European notion. Indeed, in the US, fair use covers any activity that can lawfully be undertaken without the consent of rightholders, whereas the UK notion of "fair dealing" is more stringent, as there are very few exceptions. France just refers to "*exceptions au Droit d'Auteur*" and Germany relies on the concept of "*Schranken*" (barriers) to owner controls[110]. In the following developments, the notion of "fair use" will be used as a "generic" expression to refer to any exception to owners' rights in favour of lawful users, whatever the country of implementation is. Indeed, in any case, DRM undermines fair users' rights (1) to transform them into a new kind of right of access to works (2). It has also consequences on public domain (3).

1. Decreasing exceptions to copyright

Once again, the most apparent danger comes from TPM (a), but RMI also presents risks to take into account (b).

a) TPM at odds with fair use

[109] Christophe Geiger, "Copyright and free access to information: for a fair balance of interest in a globalised world" *European Intellectual Property Review 2006*, 28(7), p.369
[110] Martin Kretschmer, op. cit. p.337

To understand the issue with TPM, it is necessary to analyse the scope of fair use with regard to TPM (i) and circumvention (ii). Then, issues about the private copying exception (iii) and fair use in online environments (iv) must be highlighted, before giving the French and British examples of implementation (v).

i. Fair use in spite of TPM

According to article 6(4)§1 of the ISD, despite the protection of TPM against circumvention established in article 6(1), rightholders may take fair use into account. When rightholders do not take voluntary measures in that way, Member States "*shall take appropriate measures*"

to ensure that rightholders make available to users the means of benefiting from exceptions to exclusive rights of copyright holders implemented in their national law, and given that users have legal access to the protected work or subject-matter concerned.

Article 6(4) does not provide for exceptions to article 6(2) and only intends to combine the protection established in article 6(1) with exceptions to exclusive rights from article 5. The notion of "legal access to the protected work" implies that the user intends to exercise his exception on a lawful source (he has for instance bought) that is not in itself an infringing copy.

Exceptions concerned are an exhaustive and quite limited list of optional exceptions. It concerns exceptions to reproduction right, as provided for in articles 5(2)(a) relative to

reproductions on paper, 5(2)(c) relative to reproductions made by publicly accessible libraries, educational establishments, museums etc., 5(2)(d) relative to ephemeral recordings of works by broadcasting organisations, and 5(2)(e) relative to reproductions of broadcasts made by social institutions pursuing non-commercial purposes. It also concerns optional exceptions to reproduction right and communication or making available right, as provided for in articles 5(3)(a) relative to the use (reproduction and communication) for the sole purpose of illustration for teaching or scientific research, with indication of the source, 5(3)(b) relative to the use for the benefit of people with a disability and 5(3)(e) relative to the use for the purposes of public security or for the reporting of administrative, parliamentary or judicial proceedings.

All these exceptions must comply with the exigencies of the three-step test (article 5(5)). The obligation of article 6(4) only relies on Member States that have implemented the concerned exceptions in national law. Besides, the only compulsory exception of article 5(1) relative to temporary acts of reproduction that are transient or incidental and integral part of a technological process is not mentioned because already ensured by this article.

Several optional exceptions, from article 5(3)(c), 5(3)(d) and 5(3)(f) to 5(3)(o) are not mentioned. Thus, users cannot benefit from these important exceptions when the relevant works are protected by effective TPM. Indeed, Member States do not have any commitment in relation with them[111].

Finally, the private right to copy, (or private copying exception) of article 5(2)(b) is mentioned in article 6(4)§2. This exception enables a natural person to make reproductions on any medium for private use, for ends that are neither directly nor indirectly commercial, and provided that "*the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned*" (three-step test). According to article 6(4)§2, Member States "*may also take*" measures in respect of users to benefit from the reproduction for private use, unless it has already been made possible by rightholders, and "*without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions*".

Contrary to paragraph 1, article 6(4)§2 does not include an obligation for Member States that have implemented a private copying exception to make it compatible with TPM. Article 6(4)§2 only states: "*they may also take"* measures, whereas article 6(4)§1 states: "*Member States shall take appropriate measures*" with regard to other optional exceptions.

It is significant to assess the place of the private copying exception in the ISD. It is the only exception to rightholders' exclusive rights that is likely to concern every user (not only scientists, teachers, journalists etc.). However, Member States are not forced to implement it. If they do so, they are not forced to ensure its effective utilisation in the face of TPM, and if they do so, they cannot prevent rightholders from limiting its scope to a certain number of reproductions.

ii. Fair use as a kind of circumvention

The balance between exclusive rights of rightholders and lawful exceptions to these rights is really threatened. Indeed, TPM are likely to curb the possibility for users to benefit from their exceptions. It is what we call "the digital lock up". Therefore, users will have two

[111] Terese Foged, op. cit. p. 537

choices: either they sue rightholders in order to exercise their exceptions, or they try to circumvent the TPM[112]. Anyway, they cannot obtain circumvention devices as trafficking is also prohibited. Dr Jacques De Werra (University of Geneva) explained the situation as follows: "*The user (because of the exemption) has now gained the right to unlock the door of the room where the work is located, but no locksmith has the right to develop and give/sell her the tools (i.e. the key) that she could use to unlock the door (or to open the door for her). As a consequence, if she cannot do it herself, the user cannot practically benefit from the exemption.*"[113]

But even if they do it themselves, are users allowed to circumvent TPM in order to perform a lawful exemption to exclusive rights? Or can they be prosecuted for circumvention, even if they did not commit any copyright infringement, and even if they do not want to commit one? The problem is that TPM are blind and cannot discern between lawful users and potential infringers[114].

So users will be punished for any circumvention whatever the objective pursued was, even in the absence of any copyright infringement, even to utilise a right that is ensured by law. It is quite logical given that circumvention has to be distinguished from copyright infringement. Moreover, it transpires from article 6(4) that despite the safeguards ensured by states relatively to exceptions, TPM prevail over them. The exercise of an exception excuses neither an act of circumvention nor an act of trafficking in circumvention devices.

Furthermore, Member States only ensure utilisation of exceptions "*in the absence of voluntary measures taken by rightholders*" that make available "*the means of benefiting from that exception*" (article 6(4)). So, rightholders are granted legitimacy in controlling traditional copyright exceptions by means of technology[115]. As Dr Severine Dusollier (University of Namur) explains, "(...) *anti-circumvention provisions address any use that technology can encapsulate and consider exceptions and fair use as nothing but failures of the copyright body that technology can heal*"[116].

---

[112] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.292

[113] Jacques de Werra "The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)" p.21 *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/Reports/dewerra.doc

[114] Christophe Geiger, op. cit. p. 369

[115] Severine Dusollier, "Technology as an imperative for regulating copyright: from the public exploitation to the private use of the work" *European Intellectual Property Review 2005*, 27(6), p. 203

[116] ibidem.

iii. The private copying exception in its death throes

As already evoked, the private copying exception is likely to concern everyone. Researchers need to inform themselves about the current state of science by copying different sources (and not only for purposes of illustration), and authors, before being authors of a work, are mere users. To undermine this exception is, to a certain extent, to undermine creation[117].

Nevertheless, private copying mainly remains a consumer exception, part of privacy and freedom of expression. All benefits of this exception are likely to be hindered by TPM.

On this point, the U.S DCMA[118] is more favourable than the ISD, given that it distinguishes between "access control" measures and "copy control" measures. Trafficking in devices enabling the circumvention of access control measures and copy control measures is equally prohibited (sec.1201 (a)(2) and (b)). However, only the circumvention of TPM "*which effectively controls access to a work*" is prohibited under section 1201 (a)(1)(A). So, this system takes into account fair use, contrary to the ISD one: under the DCMA, a user is indirectly entitled to circumvent a copy control device in order to exercise his private copying exception. In practice, it could make copy control devices completely useless. But in the case where an access control device also prevents the exercise of a copying exception (no access, so no way to copy), users cannot circumvent it.

[117] Christophe Geiger, op. cit. p. 371

[118] The Digital Millennium Copyright Act (1998) http://thomas.loc.gov/cgi-bin/query/F?c105:6:./temp/~c105TjnYFD:e884:

So, this tolerance concerning copy control is perhaps a mere smoke screen. In any event, it requires a technically skilled user to circumvent such devices[119]. True pirates are able to circumvent most devices, not average users. So TPM are likely to hinder fair use, not to harm piracy at all[120].

Anyway, in the EU, circumvention is already prohibited whatever the purpose is. A famous example of this intransigence is the French case called "*Mulholland Drive*". A person wanted to reproduce on videotape a DVD of the movie "*Mulholland Drive*" he had bought, in order to watch it on his parents' VCR (expecting to enjoy both his private copying exception and interoperability with old devices). The reproduction was impossible due to a copy control device. He made a complaint because his private copying exception was hindered. The *Tribunal de Grande Instance* of Paris held that he had no right to copy a movie adapted on a digital media support because it would be detrimental to the normal exploitation of the work. It referred to the Berne three-step test (article 9(2) of the Convention)[121].

The Court of Appeal of Paris invalidated this decision on the grounds that the reproduction of a work on a digital support was not damaging to the normal exploitation of the work concerned, and explaining that the private copying exception concerned all types of media[122]. The Court of Cassation finally invalidated the Court of Appeal's decision by holding, in the light of the ISD that: "*Any infringement caused to the normal exploitation of a work likely to turn down the exception of private copying must be assessed by taking into account not only the inherent risks to the new digital environment as far as the protection of authors' rights are concerned, but also the economic consequences the exploitation of that DVD can have on the movie production costs*"[123].

This decision proves that the three-step test is not only the concern of lawmakers, but must be assessed for each utilisation of an exception such as the private copying one[124]. It above all gives an economic approach to the private copying exception, which is thus bound by the exploitation of the work concerned, according to the methods of sale, rentals, and according to the threat of the digital environment.

However, it is hard to know whether the solution would have been different with another type of work, such as an audio CD, or with another work of the same type (another movie)[125]. Anyway, it is a good example of the effects of TPM on fair use. The recent decision of the

[119] Nora Braun, op. cit. p. 497
[120] Kamiel J. Koelman, op. cit. p. 278
[121] TGI Paris (3° ch., 2° sec.) 30 April 2004
[122] Cour d'Appel de Paris (4° ch.) 22 April 2005
[123] Cour de cassation (1° ch.), 28 February 2006, *s.a. Studio Canal, s.a.s. Universal Pictures Vidéo France et Syndicat de l'édition vidéo c. M. Perquin et association U.F.C.-Que choisir*
[124] Laurier Yvon Ngombe "Technical measures of protection versus copyright for private use: is the French saga over?" *European Intellectual Property Review 2007*, 29(2), p.63

Court of appeal on this case confirms that the private copying exception must not be regarded as a right. It must be considered to be a mere exception that can be raised by users to defend themselves against complaints relative to infringements[126]. Such decisions certainly raise another issue given that levies still exist on blank supports and hard disks to compensate for the private copying exception. So, should they logically disappear?

iv. The undermining of fair use in online environments

The first paragraph of article 6(4) tries to combine public policy exceptions (education, libraries etc.) and TPM by providing for positive obligations for Member States concerning a limited range of exceptions. The second one narrows down the private copying exception at the discretion of states. And the last step is the fourth paragraph which states: "*The provisions of the first and second subparagraphs shall not apply to works or other subject-*

[125] Bernard Lamon "Affaire '*Mulholland Drive*': la copie privée sérieusement limitée" *Journal du net* (2 March 2006) http://www.journaldunet.com/juridique/juridique060303.shtml

[126] Cour d'appel de Paris (4° ch. section A) 4 April 2007 *UFC Que Choisir, M. Perquin c. Films Alain Sarde and others*

matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them".

It concerns the Internet, the online environment, where the making available of contents on agreed contractual terms is involved: there is only a right of access to the contents[127]. In such a context, the Member States' positive obligations of article 6(4)§1, and the incentives of article 6(4)§2 disappear.

Different services can correspond to the description given such as on-demand services or streaming[128]. So these services may be excluded from the positive obligations of article 6(4)§1 and from the conditions of article 6(4)§2. However this kind of services probably represents the future of consumption of copyrighted works.

It will spread to the detriment of traditional works with copy control systems, where exceptions are eventually better guaranteed under article 6(4)§1 and 2 of the ISD, or where circumvention is almost tolerated under the DCMA.

Furthermore, the expression "agreed contractual terms" may also be seen as a contractual escape from the potential obligations of rightholders under article 6(4)§1 and 2. Indeed, as soon as rightholders are covered by "agreed contractual terms", Member States cannot ensure that they make users benefit from their exceptions anymore. Such contracts are rightly used in on-demand services or in softwares licensing. They are often called "click-wrap" or "browse-through" licences and state that by using the contents, the user agrees to abide by the terms of the licence (refraining fair use)[129]. They are some kind of membership agreements, and users have no choice.

So there is a double punishment, these agreements are at odds with fair use, and moreover, according to the fourth paragraph of article 6(4), their very existence prevents Member States from ensuring fair use.

v. The French and British examples: a confirmation of the undermining

A true clarification could come from implementations in domestic law. However in French law, the new provisions of August 1st, 2006[130]do not clarify the scope of article 6(4) of the ISD. The new Regulatory Authority for Technical Measures ("ARMT") now ensures users' exceptions according to article L331-8 of the Intellectual Property Code ("CPI"). In the

[127] Nora Braun, op. cit. p. 501
[128] cf technical glossary p.72
[129] Terese Foged, op. cit. p. 525 and 538
[130] Loi n° 2006-961 of 1 August 2006 "*relative au droit d'auteur et aux droits voisins dans la société de l'information*" *Official Journal* n° 178 of 3 August 2006, page 11529, called "DADVSI"

absence of decisions taken by rightholders, or when there is a conflict between them and users, the ARMT can determine how exceptions shall be utilised, and how many copies can be made according to the type of work or subject-matter, the methods of communication to the public, and according to the TPM concerned.

However, like in the ISD (article 6(4)§4), article L331-10 provides that rightholders do not have to enable users to benefit from their exceptions when the work is made available according to "agreed contractual terms" in such a way that members of the public may access them from a place and a time individually chosen by them.

The new rules are quite the same in the UK. Section 296ZE of the Copyright and Related Rights Regulation[131] provides for remedies when effective TPM prevent permitted acts (domestic exceptions for lawful users). Thus, paragraph (2) states: "*Where the application of any effective technological measure to a copyright work other than a computer program prevents a person from carrying out a permitted act in relation to that work, then that person or a person being a representative of a class of persons prevented from carrying out a permitted act may issue a notice of complaint to the Secretary of State*". This authority will then play a role similar to the French ARMT in ensuring that rightholders respect user's exceptions. The main difference is the absence of private copying exception ensured by law. Anyway, paragraph (9) states that section 296ZE does not apply to works "*made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them*".

These provisions are nothing more than a "copy/paste" of the fourth paragraph of article 6(4), without any clarification of the actual scope of the limitation. We still do not know which services and which contracts are really concerned[132].

b) The risks relative to the definition of RMI

Article 7 of the ISD does not refer to users' exceptions, and indeed RMI is not supposed to curb the utilisation of such exceptions. It only includes information devices, and not protection devices. So users, when performing a private copying exception or a studying exception should leave digital marks intact on the works they use. And the marks may outlive the copy.

[131] The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003 (amending the CDPA of 1988)

[132] Michael Hart and Steve Holmes, op. cit. p.256

However, the frontier between RMI and TPM is not so clear, and technical features that enable an actual tracing of consumption patterns go beyond mere information. Some devices straddle RMI and TPM, identification and protection, like for instance Electronic Copyright Management Systems ("ECMS")[133]. They are the forerunners of DRM. They enable both the identification of copyright materials and the monitoring of their usage, while rewarding rightholders with appropriate remuneration. They are hybrid systems, comprehensive systems[134].

Thus, rightholders using such devices could benefit from the definition of RMI rather than the one of TPM, in order to ensure a complete protection against removal and so evade article 6(4) provisions, which tolerate fair use[135].

2. The shift of fair use towards a mere right of limited access to works

With the implementation of DRM, fair use will evolve towards a mere right of access (a), what will change the methods of consumption of works (b).

a) The new system of licence: From a right of obtaining copies to a right of access

The implementation of DRM systems in copyright law makes traditional fair use evolve towards something more stringent for users. It is often called the "digital lock up", given that it undermines fair use, it locks up users into proprietary formats which restrict interoperability, etc.

However, the lock up should not be more favourable to rightholders given that their main interest is rightly to distribute and make available their content to consumers to the widest extent possible[136].

Anyway, it does not prevent them from changing users' methods of use and access to works. Traditionally, copyright licences to users were close to a right to get copies of works. It was implied that users had a certain liberty to do what they wanted with their copies in their private sphere. Today, reproduction is controlled, and above all, access to works is

[133] cf technical glossary p.72
[134] cf. http://www.ariadne.ac.uk/issue2/copyright/ and http://www.ariadne.ac.uk/issue21/ecms/
[135] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.297
[136] Nora Braun, op. cit. p.502

controlled. Since reproduction devices enable perfect digital copies, rightholders are more distrustful. In most Member States, reproduction is now allowed for only one or two private copies[137], or even none like in the UK.

Through the protection of DRM systems against circumvention, a right of access to works has been introduced in copyright law. Indeed, according to article 6(3) of the ISD, TPM are protected when they are effective, in particular, "*where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control*". So access control is protected against circumvention, and any user who obtains access without authorisation may be prosecuted.

There is clearly a change in the perception of copyright. It traditionally protected authors against commercial exploitation performed by potential competitors rather than acts performed by end-users, by consumers. In the digital environment, a new perception of copyright will consist in granting consumers a limited right of access[138]. In the immediate future, users will not pay for copies, but for a determined use that will be more and more characterized by a right of temporary copy (streaming, video-on-demand etc.). When it will be strongly restricted, will we still talk about fair use?

b) The future of consumption of copyrighted works

In the future, consumers will be able to access any work, at any moment, but never to get their own copy. It will constitute a psychological change for thousands of consumers who did not buy works only to read them, play them etc., but also as collectors, to possess hard copies of works[139].

In practice, access rights could consist in obtaining a digital copy of a work with TPM preventing any access. To read or play the work, users would have to acquire a digital key, which may vary according to the right of access granted (how many uses, how many copies permitted, for how long etc.). And thanks to RMI, the key would identify both the work and the rights granted to users (conditions of licence), and perhaps users themselves.

As soon as users will have a restricted access right, fair use will not be guaranteed anymore. Indeed, article 6(4) of the ISD is intended to guarantee users' exceptions to copyright in spite of TPM, "*where that beneficiary has legal access to the protected work or subject-matter*". So, fair use is dependent from a right of access: no right of access, no fair use. This right is

[137] ibidem. p.501-503
[138] Kamiel J. Koelman, op. cit. p. 275
[139] Jane C. Ginsburg "From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law" *Journal of the Copyright Society of the USA* (Vol. 50, 2003), p.114 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493

ensured by DRM measures which can clearly define what users can do and what they cannot do, according to agreed contractual terms (article 6(4)§4). In such a context, exceptions to rightholders' monopoly as ensured by national law will probably outlive their usefulness.

Another problem will appear if the right of access focuses on users' devices. DRM systems will allow them to use certain works on a particular computer, or will recognise computers thanks to their IP address[140] or configuration. What if these elements change? Will the copies of works still work? Will the works still be accessible with the same codes? It is very close to the broader question of interoperability.

A recurrent argument in favour of this new regime is the one of price discrimination: thanks to new methods of consumption, the use of works may cost less given that people may consume and pay according to their needs and wishes[141]. On the contrary, until now, users have had to acquire copies, and so to pay for everybody's fair use even if they did not expect to make copies of works. For instance, the price of a CD was the same for each user. Moreover, everybody had to pay levies on blank discs whether they expected to benefit from private copying exceptions or not.

In the future, with new rights of access, a consumer wanting to listen to a song twice could pay proportionally less than a person wanting to listen to this song five times, or to make one or several reproductions of it. Nevertheless, fair use costs were traditionally chargeable to rightholders, not users, as soon as there was fair compensation[142]. As a result, a new right of access could significantly increase the cost of copies allowing a relatively free use. In practice, it may curb scholarly or critical examination of works, where copies are currently obtained from public libraries, for a reasonable price, and with quite broad fair use possibilities (illustration, reverse engineering etc.)[143].

Furthermore, beyond consumers, new methods of consumption may certainly cause an economic turmoil for sectors of industry specialised in reproduction devices, from recorders to blank media[144].

[140] cf technical glossary p.72
[141] Nora Braun, op. cit. p.502
[142] Jane C. Ginsburg, op. cit. p. 113
[143] ibidem. p.117
[144] Philippe Andrieu "Les mesures techniques de protection" *Encyclopédie Juridique des Biens Informatiques*, p. 13 http://encyclo.erid.net/document.php?id=318#ftn14

3. The question of public domain

Finally, DRM raises issues relative to public domain: TPM may lock up works in the public domain. Indeed, TPM are protected against circumvention as soon as they are "*designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder*" (article 6(3) of the ISD).

Does it mean that protection is required as soon as the technology was initially designed to prevent any activity prohibited under copyright (or database) law, regardless of whether it actually protects copyright or not? In such a case, circumvention must also be unlawful when a device initially designed to protect copyrighted works actually protects public domain works[145]. So, there should be no public domain anymore.

In fact, it depends on the definition of "designed to". It could be perceived as "created in order to" or as "used in order to". Anyway, the French implementation seems to exclude this

[145] Kamiel J. Koelman, op. cit. p. 273

possibility because it states "*destinées à*" (L331-5 CPI), what means "intended for" rather than "designed to". A meaning close to the notions of "aim" and "use" should be preferred rather than a meaning close to the notions of "creation", "invention". Indeed, with the latter meaning, the circumvention of devices preventing access to public domain content is very likely to be prohibited. The victims of such a system would have to deal with it, or to address a complaint to the Secretary of State in the UK or to the ARMT in France.

Anyway, nothing in the ISD ensures access to public domain content protected by TPM. Whether or not circumvention is tolerated in such a case, nothing is provided for "unlocking" works protected by TPM when they fall in the public domain. Indeed, all users would not have the necessary skills to circumvent such devices, even if it was tolerated. Nevertheless, TPM will probably not be able to protect works for so long (70 years after the death of the author), as technology will still evolve[146].

Another problem may appear in the case where a same TPM protects both copyrighted content and public domain content. While protecting copyrighted content, the devices will also prevent lawful access to other content[147]. So, the protection of public domain works by TPM should have been clearly prohibited by the ISD. This is also an aspect of the digital lock up, given that the possibilities for users are thin. Indeed, they cannot address complaints to their national authorities when it deals with the Internet, given that according to article 6(4)§4, safeguards do not apply when works are made available on agreed contractual terms in an online environment[148].

So, for example, no defences could be raised in the case of the *Adobe*'s eBook DRM, which disallowed printing, copying, content extraction for accessibility (and especially to read the book aloud!) and commenting on *Alice in Wonderland* by Lewis Carroll, although it was a public domain work[149].

Anyway, new methods of consumption and effects on public domain are only copyright-focused problems. Now, beside fair use issues, DRM is likely to cause collateral damage to users.

---

[146] Barry B. Sookman, op. cit. p. 157

[147] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.294

[148] Colin Nasir "Taming the beast of file-sharing – Legal and technological solutions to the problem of copyright infringement over the Internet: part 2" *Entertainment Law Review 2005*, 16(4), p.88

[149] Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.161

Section B. Quis custodiet ipsos custodies?[150]: DRM's collateral damage to consumers

Beyond fair use, effects of DRM have to be assessed, in particular as regards freedom of expression (1), privacy (2), interoperability (3) and innovation (4).

1. The danger of DRM regarding freedom of expression

Undermining fair use is more or less directly undermining scientific research, artistic creation, journalism, criticism etc. All these purposes are linked with the fundamental notion

[150] Juvenal, *Satire VI*, translated as "Who will guard the guards?".

of "freedom of expression". Despite DRM, the ISD is supposed to ensure freedom of expression. Indeed, recital (3) states: "*The proposed harmonisation* (...) *relates to compliance with the fundamental principles of law* (…) *including* (...) *freedom of expression and the public interest*", and recital (14) states: "*This Directive should seek to promote learning and culture by protecting works and other subject-matter while permitting exceptions or limitations in the public interest for the purpose of education and teaching*".

However, freedom of expression and in particular free speech is endangered, especially because of anti-trafficking provisions. Thus, the US case *Felten v. Recording Industry Assoc. of America* ("RIAA")[151] gives us an example that can be transposed to the EU situation. Professor Edward Felten and his research team broke a copy prevention system on music files and then published and presented their research. They were threatened of prosecution by the RIAA, but they sued for a declaratory judgment. Indeed, they estimated that the US First Amendment relative to free speech covered them. They eventually evaded sentences, but there is still a threat for their other works[152]. Scientific research relative to DRM is therefore threatened, given that scientists cannot freely publish or communicate their work.

Similarly, private copying is an essential access key to information, and so to freedom of expression. Private reproduction enables new creations, which are forms of expression. But with the DRM era, this scheme will be significantly hindered[153].

Furthermore, as article 6(4) of the ISD is only aimed at exceptions to article 6(1), it does not cover circumvention devices or services. So dealing or communicating with such devices is always unlawful, even when the devices could make users benefit from exceptions authorised by article 6(4). Users cannot get devices or information necessary to benefit from their lawful exceptions. But the right to freedom of expression includes, according to article 10(1) of the European Convention on Human Rights ("ECHR")[154] the right to "*receive and impart information and ideas*". So, according to article 10(2) of the ECHR, are the restrictions to the right to freedom of expression "*necessary in a democratic society*" in such a case?

As required, it is clearly "*prescribed by law*", but does it achieve one of the legitimate aims such as public safety, national security, authority and impartiality of the judiciary? Anti-circumvention measures are intended to protect copyright. So, it corresponds to the legitimate aim of "*the protection of the reputation or the rights of others*" provided for in

---

[151] *Felten v. Recording Industry Assoc. of America*, 6 June 2001, U.S. District Court for the District of New Jersey, Case no. 01 CV 2669

[152] Robin D. Gross "Digital Millennium Dark Ages- New Copyright Law Used to Threaten Scientific Research" (Nov. 7, 2001) - Electronic Frontier Foundation (EFF) http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011107_eff_felten_article.html

[153] Christophe Geiger, op. cit. p. 371-372

[154] European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") of 4 November 1950

article 10(2) of the ECHR. Concerning the notion of "necessity in a democratic society", it corresponds to a "*pressing social need*" and has to be "*proportionate to the legitimate aim pursued*"[155].

According to Dr Patricia Akester (University of Cambridge), the case law of the European Court of Human Rights suggests that freedom of expression could prevail on the protection of rightholders when users cannot benefit from exceptions listed in article 6(4) of the ISD. It would concern especially users who are not able "*to take advantage of existing exceptions that would grant them access to political, artistic, literary or journalistic speech*"[156]. To sum up, we could consider that, according to article 10(2) of the ECHR, anti-circumvention measures should tolerate users' freedom of expression concerning their lawful exceptions to copyright owners' rights, even if it could have negative effects on the protection of rightholders.

2. The danger of DRM regarding privacy

DRM is very close to the notion of privacy (a), and has particular effects on personal data protection (b).

a) The links between DRM and privacy

Pr Lawrence Lessig (Standford University) explains that copyright and privacy have a similar story, given that "*With both, there's a bit of 'our' data that 'we've' lost control over. In the case of copyright, it is the data constituting a copy of our copyrighted work; in the case of privacy, it is the data representing some fact about us. In both cases, the Internet has produced this loss of control: with copyright, because the technology enables perfect and free copies of content; with privacy* (...) *because the technology enables perpetual and cheap monitoring of behaviour*"[157]. What if the question of privacy monitoring is not only raised for national security purposes, but also for copyright protection purposes?

Privacy is "*the limit the law placed upon the ability of others to penetrate your private space*"[158]. It is as well as freedom of expression protected by the ECHR (article 8) which

[155] *Silver v. United Kingdom*, 25 March 1983, Series A, No. 61, (1983) 5 EHRR 347, § 97
[156] Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.161-162
[157] Lawrence Lessig *Code* – Version 2.0 (Basic books 2006) p. 200 http://pdf.codev2.cc/Lessig-Codev2.pdf
[158] ibidem.

allows strict exceptions for public authorities to interfere, when it is "*necessary in a democratic society*".

Traditionally, copyright put up with privacy, for example, the publication of materials in which persons are portrayed is restricted[159]. Moreover, to a certain extent, fair use must be ensured as a private sphere within copyright protection[160]. Nevertheless, in the digital environment, and with the development of DRM, things have changed.

DRM now raises personal data protection issues. Indeed, as an online shopping tool, DRM has the potential of amassing data about persons who purchase works or even browse works on the Internet: Name, address, IP address, tastes etc. It can foresee consumers' choices, it

[159] CDPA 1988 Sec. 85(1)
[160] Lee A. Bygrave, op. cit. p.51

enables targeted advertising, and information can be sold to other firms or entities that can eventually "*inhibit the expression of non-conformist opinions and preferences*"[161], just like a "digital panopticon"[162]. Above all, it can be used to prevent copyright infringement, as information relative to users can be included in a copy of a work, for instance by means of digital watermarking[163]. So it can trace potential infringers, for example if a work is later found on a file-sharing network[164]. This certainly harms privacy.

[161] ibidem. p.53
[162] cf. Jeremy Bentham *Panopticon* (1787 – published in 1791)
[163] Catherine Stromdale "The problems with DRM" *Entertainment Law Review 2006*, 17(1), p.5
[164] Patricia Akester, op. cit. p. 163

b) The threats to personal data protection

Recital 57 of the ISD states that RMI may "(…) *process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means, in their technical functions, should incorporate privacy safeguards in accordance with 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 the free movement of such data*". Furthermore, article 9

states that the ISD shall be without prejudice to provisions relative to data protection and privacy.

So DRM, and especially RMI, must respect the personal data protection directive ("PDP") of 1995[165]. This directive protects personal data (name, address, identification numbers, personal information etc.) against unlawful processing, and gives rights to persons concerned by lawful processing. However, nothing in the ISD enables users to circumvent TPM or RMI when the protection of their personal data is threatened.

Concerning TPM, the US DMCA is more favourable to users. According to section 1201(i)(1), the circumvention of TPM is permitted when the TPM on the work protected has the capability to collect or disseminate personal data reflecting the online activities of a natural person who seeks to gain access to the work ((A) and (B)), and when the act of circumvention has the sole effect and purpose of identifying and disabling this capability ((C) and (D)). However, the scope of this provision is unclear. We do not know if it allows the circumvention of data processing aspects of any TPM, or only the circumvention of mere cookies, which are not directly designed to protect copyright[166].

In practice, the application of the ISD while respecting the PDP may raise problems if information is collected without the consent of the user, so contrary to the provisions of article 7 of the PDP. Nevertheless, when the data processing is necessary for the performance of a contract to which the person is party, the user do not have to give his consent to the processing (article 7(b) of the PDP). So, according to article 6(4)§4 of the ISD, in the face of "*agreed contractual terms*" in the online environment, the consent of the user will not have to be obtained.

But a question remains: if TPM are exclusively designed to protect copyright by collecting users' data, do they still correspond to the definition of article 6(3) of the ISD? Are they still protected against circumvention under article 6(1)? Indeed, to be protected, TPM must be effective, and to be effective they must apply "*an access control or protection process*". It would not be the case if they only collected and processed data. So they could logically be circumvented[167].

Concerning RMI, it can be a threat as soon as it includes metadata relative to conditions of use of works. So it can process data relative to users, their identity and their consumption habits, as recital 57 implies. Users are not allowed to remove them, even to protect their

---

[165] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal* L 281, 23.11.1995, p. 31–50

[166] Lee A. Bygrave, op. cit. p.55

[167] Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.296

personal data. Once again, the DCMA is more favourable as section 1202 excludes from protected RMI digital information used for monitoring usage of copyrighted works.

On the other hand, Recital 57 also encourages RMI that respects the PDP, that is to say Privacy-Enhanced Technologies ("PET"). An example of such technologies could be identification numbers for legally acquired digital copies that do not identify the purchaser. Of course, there would be a link between these numbers and the purchaser, but it would remain secret. The databases holding this link would only be accessible by certification authorities, only able to supply information to law enforcement authorities[168]. This would be safer than the present databases holding the link between IP addresses and Internet users. Indeed, Internet Service Providers ("ISP") store these data whereas they are not certification authorities[169].

[168] Patricia Akester, op. cit. p. 163

[169] article 12(2) of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal* L 178,17.7.2000, p. 1–16

Anyway, despite the incentives of Recital 57, the ISD does not encourage the use of PETs in DRM. Moreover, nothing is mandatory in such a recital. So, the main problem remains the uncertainty about the application of both directives, according to the balance between copyright protection and personal data protection[170].

However, electronic commerce can only develop if consumers do not fear for their privacy. And as copyright needs electronic commerce to be promoted in the digital environment, DRM has to respect users' privacy while protecting copyright[171].

[170] Lee A. Bygrave, op. cit . p.56-57
[171] ibidem. p.57

3. The thorny question of interoperability

The interoperability issue is maybe the main criticism levelled against DRM (a), and this problem has also notable consequences on competition between industries (b).

a) The lack of interoperability in DRM

The debate relative to DRM's interoperability is, as already evoked, often linked with *Apple*'s businesses, and in particular in France. If Recital 54 of the ISD encourages (recitals do not enforce) "*compatibility and interoperability of the different systems*", it only concerns interoperability among DRM systems, and not interoperability of DRM systems with other devices, such as music or video players, computers etc.

However, both types of interoperability must be improved. On the one hand, the lack of interoperability between DRM systems prevents for instance users from playing *Sony*'s *ATRAC* protected files on *Apple*'s *iPods* players, and vice versa. But on the other hand, none of the DRM protected files can be played on free-softwares players, or under *Linux*. Moreover, some copy control systems on audio CDs also prevents users from playing them on common stereo systems or car audio players. On the contrary, sometimes it can only be played on these devices and not on PC CD players[172].

Anyway, if the ISD does not ensure interoperability, it does not prohibit it either. Indeed, the anti-circumvention provisions of article 6(2) do not prevent in the absolute the development of compatible devices able to play several or all proprietary DRM standards. Compatibility is not circumvention[173].

Once again, the US DCMA is more favourable and includes a mandatory provision (section 1201(f)) to ensure reverse engineering for the purpose of interoperability between software components (e.g. DRM files with music players, and vice versa). It is closer to article 6 of the EC Software Directive[174]. However, these provisions are aimed at competitors, not users.

France went further by voting for explicit DRM interoperability provisions, what *Apple* called the "*state-sponsored piracy*"[175]. Initially, users had the possibility to request interoperability information from DRM providers, and a court could order the provider to release it. Only information transmission charges could be applied and no royalties. Moreover, DRM providers could not prevent the publication of the source code of interoperable computer programs.

Nevertheless, the present provision (the one that applies), is more lenient, and only states that TPM must respect interoperability (L331-5§4 CPI), and that DRM providers must give information that is essential to interoperability, according to articles L331-6 and L331-7. These two articles provide that the ARMT mediates interoperability requests according to a specific procedure. Even if it can apply fines, DRM providers can evade interoperability

[172] Terese Foged, op. cit. p. 528
[173] Mikko Valimaki and Ville Oksanen, op. cit. p.563
[174] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17.5.1991, p. 42–46
[175] Tom Braithwaite "France approves law to challenge Apple" *Financial Times* (Mar 21, 2006) http://search.ft.com/ftArticle?startDate=27%2F02%2F2006&dsz=1&dse=true&queryText=apple&endDate=02%2F04%2F2006&activeTab=ftNews&aje=false&resultsToReturn=10&id=060321009950 and Jean Philippe Hugot and Olivier Hugot "The DADVSI code: remodelling French copyright law for the information society" *Entertainment Law Review 2006*, 17(5), p.144

requests if there is "*a security risk that TPM become inefficient*". Thus, interoperability measures are likely to be quite useless.

However, the lack of interoperability certainly leads to unlawful circumvention. So the objective of copyright protection is not reached anymore[176]. That is why the EC communication on "Management of Copyright and Related Rights in the Internal Market" of 2004 encouraged interoperability of systems in the EU. It highlighted the need to find open standards of DRM to safeguard the public interest[177].

Obviously, Steve Jobs (CEO of *Apple*) tried to qualify the impact of interoperability on public interest, by explaining that proprietary formats (like *Apple*'s ones) did not create the alleged "digital lock up". Thus he explained: "*Through the end of 2006, customers purchased a total of 90 million iPods and 2 billion songs from the iTunes store. On average, that's 22 songs purchased from the iTunes store for each iPod ever sold. Today's most popular iPod holds 1000 songs, and research tells us that the average iPod is nearly full. This means that only 22 out of 1000 songs, or under 3% of the music on the average iPod, is purchased from the iTunes store and protected with a DRM. The remaining 97% of the music is unprotected and playable on any player that can play the open formats. It's hard to believe that just 3% of the music on the average iPod is enough to lock users into buying only iPods in the future. And since 97% of the music on the average iPod was not purchased from the iTunes store, iPod users are clearly not locked into the iTunes store to acquire their music*"[178].

Whatever the pertinence of these figures is, we can still regret that all digital works, and even technically protected ones, cannot be freely played on any device or software. Indeed, most of them have been lawfully accessed, and fair compensation has often been duly paid. Now, in the digital age, "*all parts of the media centre must operate seamlessly with each other*"[179].

Similarly, the lack of interoperability is linked with the hindering of private reproduction possibilities. It is quite paradoxical in the digital environment where most actions imply reproduction of files. Those reproductions are more or less temporary, but in most cases they are indispensable to use works on common devices[180].

[176] Patricia Akester, op. cit. p. 164
[177] COM/2004/0261 final - 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, 1.2.5, p. 10
[178] Steve Jobs, op. cit.
[179] Mikko Valimaki and Ville Oksanen, op. cit. p. 562
[180] Philippe Andrieu, op. cit. p. 13

b) Interoperability and competition

As interoperability corresponds to compatibility, there is also a risk of lock up for industrials. Indeed, some actors can grant licences on technical standards to industrials under their own conditions, and sometimes in spite of competition rules. It is the case when a company in a dominant position owns a key standard, and refuses to license competitors to develop this standard, like in the IMS health case[181].

According to the Magill decision[182], an abuse of a dominant position (article 82 of the EC Treaty) is constituted when the refusal to grant a licence prevents the creation and marketing of a new substitute for which there is potential consumer demand (1), when there is no justification for the refusal (2), and when the refusal monopolises a separate secondary market and thus causes potential losses to consumers (3).

Such principles certainly inspired the French competition council that questioned *Apple*'s *FairPlay* DRM in relation to competition law[183]. However, the conditions were insufficient to establish a compulsory licensing of information about DRM interoperability to competitors[184]. Anyway, nothing guarantees that competition law is an appropriate pattern of rules to regulate interoperability. It is probably more adequate to regulate it by means of consumer law, because interoperability is not only harmful when it deals with companies that are in a dominant position.

The problem of interoperability may just be another example of opposition between intellectual property and competition. Besides, to protect creations, to protect proprietary formats and to prevent competitors from doing reverse engineering could be regarded as something legitimate, like industry know-how protection or industry patent protection. However, this protection is wrongfully harmful for users, and it necessarily undermines innovation.

---

[181] *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* - ECJ, Case C-418/01, April 29, 2004

[182] *Radio Telefis Eireann ("RTE") and Independent Television Publications Ltd ("ITP") v Commission of the European Communities*, ECJ, Joined Cases C-241/91 P and C-242/91 P, April 6, 1995

[183] Conseil de la Concurrence *"Décision N° 04-D-54 relative à des pratiques mises en oeuvre par la société Apple Computer, Inc. dans les secteurs du téléchargement de musique sur Internet et des baladeurs numériques*" november 9, 2004.

[184] Mikko Valimaki and Ville Oksanen, op. cit. p. 566

4. The threats to innovation

The DRM threat to traditional fair use and its consequences on creation have already been evoked. By restricting the use and especially the reproduction of works, DRM curbs free criticism, comment, news reporting, scholar works, teaching and research works etc. However, progress and creation are an accumulation of different layers of knowledge that have been made available. As Isaac Newton said, "*if I have seen far it is by standing on the shoulders of giants*". But it only implies to have access to ideas of predecessors, in order to create something new. Mere copies of a work are not creations, and can become infringements[185].

Anyway, innovation as mere use may certainly be chilled. Indeed, every new use of a work will be impossible without circumvention, if the new use has not been previously imagined by rightholders. DRM will only give keys to a limited access to the work. Scientific works dealing with TPM, like for example research in cryptology, will be curbed if access to works is restricted, or if reverse engineering on works or TPM has not been allowed by rightholders.

Finally, as DRM becomes a new type of collective management of works, it is about to supplant levies. So it is likely to hinder innovation and creation for numerous artists who needed levies incomes to create works. DRM is only protection, fences. It does not enable the sharing out of funds to encourage creation and innovation[186].

[185] Barry B. Sookman, op. cit. p. 152
[186] Philippe Andrieu , op. cit. p. 13

Conclusion

To answer the question "*is DRM a necessary evil?*", we may say: "*no, it is not. If it is certainly evil, it is far from being necessary*".

The best example to illustrate this statement is probably the success of online music stores without DRM, and the abandon of DRM by several majors and industrials. Actually, it is not exactly DRM but only certain TPM that have been abandoned, and only in some areas, like music selling.

Admittedly, DRM as a balanced collective management system, used to control access to services on the Internet, and not to lock works, could be positive for everybody: users, industrials, artists. However, DRM providers would have to ensure interoperability, and would have to be careful in processing users' personal data. That is why Privacy-Enhanced Technologies should be spread.

There is a real need for auto-regulation, by artists, users, DRM providers etc. Moreover, there is a need for new innovative systems[187], like the *Creative Commons*' original systems of licensing[188]. However, even if the ISD was supposed to make room for auto-regulation, it eventually gave to rightholders an absolute power over users.

It is therefore crucial to preserve and improve the balance established by copyright. We must ensure protection for creations, but we must ensure a framework of exceptions for users as well. There must be users' rights that are not mere interests to take into account[189]. And in any case, financial compensation must be ensured, by means of statutory licences or levies[190]. Free access does not inevitably mean access for free[191].

It is only by re-establishing a real balance that social acceptance of copyright will be guaranteed. If a law is not accepted, it is unlikely that it will be respected. However, when it

[187] Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.165
[188] http://creativecommons.org/
[189] Christophe Geiger op. cit. p. 372
[190] Ibidem.
[191] F.W.Grossheide "Copyright Law from a User Perspective" *European Intellectual Property review 2001*, p. 323.

works well, copyright can provide many advantages, for creators, producers and for the whole society.

As Dr Christophe Geiger (University of Munich) explains, "*Copyright has its origins in the Enlightenment, i.e. in the recognition of the injustice of certain social dysfunctions. Today we face the same situation. It is the duty of the IP community to recognise these dysfunctions. In the agitated period before the French Revolution, the philosopher Rousseau appealed to King Louis XVI with the following words: 'If you want your laws to be observed, you have to make sure that we can love them.' When commencing the debate on an adaptation of copyright to the needs of the information society, national and international legislature should always remember these wise words of the past*"[192].

[192] Christophe Geiger op. cit. p. 373

Technical glossary

- **Automatic gain control**: "*Automatic gain control (AGC) is an electronic system found in many types of devices. The average signal level is detected and used to adjust the gain to an appropriate level for a range of input signal levels"*[193].

- **Bus encryption**: "*Bus encryption is the use of encrypted program instructions on a data bus in a computer that includes a secure cryptoprocessor for executing the encrypted instructions*"[194].

- **Code**: a method used to transform a message into an obscured form, preventing people who do not know the code from understanding what is actually transmitted.

- **Cookie**: cookies are parcels of text sent by a server to a web browser and then sent back unchanged by the browser when it accesses the server. The primary purpose is to facilitate browsing and authenticating on servers.

- **Copy-protection system**: any technical measure designed to prevent duplication of a work.

- **Cracker**: A cracker (sometimes called "pirate") is a person who modifies softwares in order to remove protection systems (and especially copy-protection systems).

- **Cryptology or cryptography**: the science of message secrecy. The purpose is to hide the meaning of messages, but not usually their existence. It uses encryption methods or mere codes.

- **Decompilation**: the act of translating a computer program into source code. It can be used for the recovery of lost source code, computer security, interoperability, error correction etc. It is close to the notion of "reverse engineering".

[193] http://en.wikipedia.org/wiki/Automatic_gain_control
[194] http://en.wikipedia.org/wiki/Bus_encryption

- **Digital fingerprinting**: a form of watermarking where hidden marks (prints) vary from person to person what enables a better tracking of the source of infringing copies of a work.

- **Digital watermarking**: a technique which allows persons to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents in order to identify content and then to control access or use of digital content.

- **Electronic Copyright Management Systems (ECMS)**: ECMS are mechanisms used to ensure copyright enforcement. It has two aspects: softwares enabling document tagging and identification of authors; and documents and softwares governing and controlling distribution of the work. Nowadays, we rather refer to the notion of "DRM", even if all recent DRM systems do not include these two aspects[195].

- **Encryption**: the process of obscuring information to make it unreadable without special knowledge or equipment (keys).

- **Interoperability:** "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*"[196]. In clear, interoperability corresponds to the compatibility of devices or softwares with other devices or softwares.

- **IP address:** an Internet Protocol (IP) address is a unique number used by electronic devices or computers to identify and communicate between them on a network (local, or global). It is a computer address which indirectly identifies computer users.

- **Key (encryption)**: A piece of information that controls the operation of an encrypted algorithm. It enables the transformation of normal text into cipher text (encrypted text) and vice versa.

- **Metadata**: Encoded data which describe characteristics of items to make them understandable. It is simply data about data. It can for example describe, associate data, or give information about other pieces of information such as titles, authors, publication date, price, serial numbers etc. to make them identifiable.

- **Reverse engineering**: "*The process of analysing a subject system to identify its components and their interrelationships to create a representation of the system in another form or at a higher level of abstraction*"[197]. It is a method that allows the

[195] http://www.ariadne.ac.uk/issue2/copyright/
[196] Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990
[197] Ibidem.

visualisation of the software's structure, of its ways of operation, in order to understand how it works.

- **Rootkit:** "*A rootkit is a set of software tools intended to conceal running processes, files or system data from the operating system. Rootkits have their origin in relatively benign applications, but in recent years have been used increasingly by malware to help intruders maintain access to systems while avoiding detection*"[198].

- **Source code:** any sequence of statements and/ or declarations written by a programmer in programming language (currently in a text file) which will be converted by the computer in a computer-executable form.

- **Streaming:** a method used to make available media, where contents are continuously received and displayed to users while they are delivered by the provider (simultaneously).

[198] http://en.wikipedia.org/wiki/Rootkit

List of references

(*In order of appearance*)

- P. Goldstein. "Copyright and Its Substitutes" *Wisconsin. Law Review* 1997. p. 865-871.
- Lee A. Bygrave, "the technologisation of copyright: implications for privacy and related interests" *European Intellectual Property Review 2002*, 24(2), p.51-57.
- Michael Flint, Nick Fitzpatrick and Clive Thorne, *a user's guide to copyright* (Tottel publishing 6th edition 2006) p. 464-472
- Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan (Trusted Systems Laboratory - HP Laboratories Cambridge), "If Piracy is the Problem, Is DRM the Answer?" *HPL-2003-110*, May 27th , 2003 http://www.hpl.hp.com/techreports/2003/HPL-2003-110.pdf
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167 , 22/06/2001 p.10 -19
- http://en.wikipedia.org/wiki/Copy_protection
- http://en.wikipedia.org/wiki/Analog_hole
- COM/1988/0172 - Green Paper on copyright and the challenge of technology - Copyright issues requiring immediate action
- B. Posner, "Purposes and scope of the Green Paper on Copyright and the Challenge of Technology", in *Copyright and the European Community: The Green Paper on Copyright and the Challenge of New Technology* (F. Gotzen ed., 1989), p.2-8.
- Martin Kretschmer, "Digital copyright: the end of an era", *European Intellectual Property Review 2003*, 25(8), p. 333-341
- *The United States Code* Title 17 "Copyright Law of the United States of America and Related Laws" Chapter 10 "Digital Audio Recording Devices and Media" § 1002. http://www.copyright.gov/title17/92chap10.html#1002
- WIPO copyright treaty, 20 December 1996 http://www.wipo.int/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf
- WIPO Performances and phonograms treaty, 20 December 1996 http://www.copyright.gov/wipo/treaty2.html
- The Digital Millennium Copyright Act (1998) http://thomas.loc.gov/cgi-bin/query/F?c105:6:./temp/~c105TjnYFD:e884:

- COM/1995/0382 - Green Paper - Copyright and Related Rights in the Information Society
- COM/1996/0568 – Commission communication -Follow-up to the Green paper on copyright and related rights in the information society
- Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.285-297
- Directive 98/84 E.C. of the European Parliament and the Council on the legal protection of services based on, or consisting of, conditional access, *Official Journal* L320, November 11, 1998 p. 54-57
- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17.5.1991, p. 42–46
- http://en.wikipedia.org/wiki/Information_society
- http://www.mises.org/content/aboutmachlup.asp
- Henning Wiese, "The justification of the copyright system in the digital age" *European Intellectual Property Review 2002*, 24 (8), p.387-396
- Charles Clark, "The answer to the machine is in the machine", *The Future of Copyright in a Digital Environment* (P. Bernt Hugenhotltz, ed., 1996), p. 139- 146.

Florian Koempel "Digital Rights Management" *Computer and Telecommunications Law Review 2005*, 11(8), p.239-242

- http://www.emimusic.info/us_EN/sect4.html
- Patricia Akester, "Survey of technological measures for protection of copyright" *Entertainment Law Review 2001*, 12(1), p.36-39
- http://www.ifpi.org/content/section_resources/isrc.html
- http://www.iswc.org/iswc/en/html/home.html
- Michael Geist "Legal fallout from Sony's CD woes" *BBC news* (3 January 2006) http://news.bbc.co.uk/2/hi/technology/4577536.stm
- Randall Stross "Digital Domain: Want an iPhone? Beware the iHandcuffs" *New York Times* January 14, 2007 http://www.nytimes.com/2007/01/14/business/yourmoney/14digi.html?ex=1326430800&en=2c5efe51f9d74dd8&ei=5090
- Loi n° 2006-961 of 1 August 2006 "*relative au droit d'auteur et aux droits voisins dans la société de l'information" Official Journal* n° 178 of 3 August 2006, page 11529, called "DADVSI"
- Nicolas Jondet "La France v. Apple: who's the dadvsi in DRMs?" *SCRIPT-ed* (Volume 3, Issue 4, June 2006) p.7-8 http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/jondet.asp

- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077 , 27/03/1996 p. 20 - 28
- L. Bently and B. Sherman, *Intellectual Property Law* (Oxford University Press 2nd edition 2004)
- Michel Vivant, Lucien Rapp, Michel Guibal, Bertrand Warusfel, Jean-Louis Bilon and Gilles Vercken, *Lamy Droit de l'informatique et des réseaux* (Lamy 2004)
- Christophe Caron, *Droit d'auteur et droits voisins* (Litec 1st edition 2006)
- Terese Foged, "US v EU anti-circumvention legislation: preserving the public's privileges in the digital age", *European Intellectual Property Review 2002*, 24(11), p.525-542
- Ketola (Afterdawn) "CSS protection used in DVDs "ineffective" Finnish court rules" (25 May 2007) http://www.afterdawn.com/news/archive/9849.cfm
- Helsinki District Court Judgment 07/4535 - 4/10 Dept. 25 May 2007 R 07/1004 http://www.turre.com/css_helsinki_district_court.pdf
- Copyright, Designs and Patents Act ("CDPA")1988 (C.48)
- *Sony Corp. of America v. Universal Studios Inc.*, 464 U.S. 417 (1984)
- *Sony Computer Entertainment UK Ltd v Gaynor David Ball & 6 Ors* [2004] EWHC 1738 (Ch)
- The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003 (amending the CDPA of 1988)
- Helen Padley, "Copyright – games – copy circumvention device (case comment)" *Entertainment Law Review 2005*, 16(1), N9
- Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, revised at Paris on July 24, 1971, and amended on September 28, 1979, article 9(2).
- Kamiel J. Koelman, "A hard nut to crack: the protection of technological measures", European *Intellectual Property Review 2000*, 22(6), p.272-288

Mikko Valimaki and Ville Oksanen "DRM interoperability and Intellectual Property policy in Europe"

European Intellectual Property Review 2006, 28(11), p.562-568

- Isabelle Vaillant "Le contournement des mesures techniques de protection, contrefaçon ou criminalité informatique ?" (June 2003) http://eucd.info/documents/transposition-eucd-2003-06-20.pdf
- Michael Hart and Steve Holmes "Implementation of the copyright directive in the United Kingdom" *European Intellectual Property Review 2004*, 26(6), p.254-257

- Christophe Caron, "Brèves observations sur la protection des mesures techniques par le droit civil*"* *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/pres_caron.doc

- Nora Braun, "The interface between the protection of technological measures and the exercise of exceptions to copyright and related rights: comparing the situation in the United States and the European community" *European Intellectual Property Review 2003*, 25(11), p.496-503

- BPI *Online Music &UK Record Industry* http://www.bpi.co.uk/pdf/Illegal_Filesharing_Factsheet.pdf

Barry B. Sookman "Technological protection measures (TPMS) and copyright protection: the case for TPMS" *Computer and Telecommunications Law Review 2005*, 11(5), p.143-159

- Tony Smith "Tiny C code bests seven-line DVD decoder" *The Register* (13 March 2001) http://www.theregister.co.uk/2001/03/13/tiny_c_code_bests_sevenline/

Tomasz Rychlicki "An opinion on legal regulations on reverse engineering and technological protections measures" *Computer and Telecommunications Law Review 2007*, 13(3), p.94-99

- Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.159-168

- C. Shapiro and H. Varian, *Information Rules: A strategic guide to the network economy* (Harvard Business School Press, Boston 1999)

- Adam Webb "It's the last rites for DRM…" *Music Week* (10 February 2007)

- International Federation of the Phonographic Industry (IFPI) *Digital Music Report* (January 2007) http://www.ifpi.org/content/library/digital-music-report-2007.pdf

- Steve Jobs "Thoughts about music" (February 6, 2007) http://www.apple.com/hotnews/thoughtsonmusic/

- Christophe Gauthier "Sans DRM, mais pas sans restrictions" *L'ordinateur individuel* (n°196 July-August 2007 p.14)
- Joel R. Reidenberg " Lex Informatica: The Formulation of Information Policy Rules Through Technology" *Texas Law Review* (Volume 76, Number 3, February 1998) p. 553-584 http://reidenberg.home.sprynet.com/lex_informatica.pdf

- articles 323-1 to 323-7 of the French criminal code or s. 1 to s.3 of the Computer Misuse Act 1990 (c. 18)

- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights *Official Journal* L 157, 30.4.2004, p. 45–86

- http://www.sppf.com/en/protectionDroits.php?PHPSESSID=54ed0e39effae6a2c653576dbb6e14df
- COM/2004/0261 final - 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
- Christophe Geiger, "Copyright and free access to information: for a fair balance of interest in a globalised world" *European Intellectual Property Review 2006*, 28(7), p.366-373
- Jacques de Werra "The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)" p.21 *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/Reports/dewerra.doc
- Severine Dusollier, "Technology as an imperative for regulating copyright: from the public exploitation to the private use of the work" *European Intellectual Property Review 2005*, 27(6), p. 201-204
- TGI Paris (3° ch., 2° sec.) 30 April 2004
- Cour d'Appel de Paris (4° ch.) 22 April 2005
- Cour de cassation (1° ch.), 28 February 2006, *s.a. Studio Canal, s.a.s. Universal Pictures Vidéo France et Syndicat de l'édition vidéo c. M. Perquin et association U.F.C.-Que choisir*
- Laurier Yvon Ngombe "Technical measures of protection versus copyright for private use: is the French saga over?" *European Intellectual Property Review 2007*, 29(2), p.61-65
- Bernard Lamon "Affaire '*Mulholland Drive*': la copie privée sérieusement limitée" *Journal du net* (2 March 2006) http://www.journaldunet.com/juridique/juridique060303.shtml
- Cour d'appel de Paris (4° ch. section A) 4 April 2007 *UFC Que Choisir, M. Perquin c. Films Alain Sarde and others*
- http://www.ariadne.ac.uk/issue2/copyright/
- http://www.ariadne.ac.uk/issue21/ecms/
- Jane C. Ginsburg "From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law" *Journal of the Copyright Society of the USA* (Vol. 50, 2003), p.113-130 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493
- Philippe Andrieu "Les mesures techniques de protection" *Encyclopédie Juridique des Biens Informatiques*, p. 13 http://encyclo.erid.net/document.php?id=318#ftn14
- Colin Nasir "Taming the beast of file-sharing – Legal and technological solutions to the problem of copyright infringement over the Internet: part 2" *Entertainment Law Review 2005*, 16(4), p.82-88
- Juvenal, *Satire VI*

- *Felten v. Recording Industry Assoc. of America*, 6 June 2001, U.S. District Court for the District of New Jersey, Case no. 01 CV 2669
- Robin D. Gross "Digital Millennium Dark Ages- New Copyright Law Used to Threaten Scientific Research" (Nov. 7, 2001) - Electronic Frontier Foundation (EFF) http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011107_eff_felten_article.html
- European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") of 4 November 1950
- *Silver v. United Kingdom*, 25 March 1983, Series A, No. 61, (1983) 5 EHRR 347, § 97
- Lawrence Lessig *Code* – Version 2.0 (Basic books 2006) http://pdf.codev2.cc/Lessig-Codev2.pdf
- Jeremy Bentham *Panopticon* (1787 – published in 1791)
- Catherine Stromdale "The problems with DRM" *Entertainment Law Review 2006*, 17(1), p 1-6
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal* L 281, 23.11.1995, p. 31–50
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal* L 178,17.7.2000, p. 1–16
- Tom Braithwaite "France approves law to challenge Apple" *Financial Times* (Mar 21, 2006) http://search.ft.com/ftArticle?startDate=27%2F02%2F2006&dsz=1&dse=true&queryText=apple&endDate=02%2F04%2F2006&activeTab=ftNews&aje=false&resultsToReturn=10&id=060321009950
- Jean Philippe Hugot and Olivier Hugot "The DADVSI code: remodelling French copyright law for the information society" *Entertainment Law Review 2006*, 17(5), p.139-144
- *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* - ECJ, Case C-418/01, April 29, 2004
- *Radio Telefis Eireann ("RTE") and Independent Television Publications Ltd ("ITP") v Commission of the European Communities*, ECJ, Joined Cases C-241/91 P and C-242/91 P, April 6, 1995
- Conseil de la Concurrence *"Décision N° 04-D-54 relative à des pratiques mises en oeuvre par la société Apple Computer, Inc. dans les secteurs du téléchargement de musique sur Internet et des baladeurs numériques*" november 9, 2004.
- http://creativecommons.org/
- F.W.Grossheide "Copyright Law from a User Perspective" *European Intellectual Property review 2001*, p. 323.

- http://en.wikipedia.org/wiki/Automatic_gain_control
- http://en.wikipedia.org/wiki/Bus_encryption
- http://www.ariadne.ac.uk/issue2/copyright/
- Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990
- http://en.wikipedia.org/wiki/Rootkit

Bibliography

(*Hypertexts links available on September 1st, 2007*)

- **Textbooks**

  - David I. Bainbridge "Intellectual property" (Pearson Longman 6th edition, 2006) p.276-278
  - L. Bently and B. Sherman, *Intellectual Property Law* (Oxford University Press 2nd edition 2004)
  - Christophe Caron, *Droit d'auteur et droits voisins* (Litec 1st edition 2006)
  - Catherine Colston and Kirsty Middleton, *Modern Intellectual Property Law*, (Cavendish publishing 2005) p. 343-347
  - Michael Flint, Nick Fitzpatrick and Clive Thorne, *A user's guide to copyright* (Tottel publishing 6th edition 2006) p. 464-472
  - Ian J. Lloyd, *Information technology law* (Oxford University Press 4th edition 2004) p. 495-506
  - C. Shapiro and H. Varian, *Information Rules: A strategic guide to the network economy* (Harvard Business School Press, Boston 1999)
  - Michel Vivant, Lucien Rapp, Michel Guibal, Bertrand Warusfel, Jean-Louis Bilon and Gilles Vercken, *Lamy Droit de l'informatique et des réseaux* (Lamy 2004)

- **Articles and reports**

  - Patricia Akester, "Digital Rights Management in the 21st century" *European Intellectual Property Review 2006*, 28(3),p.159-168
  - Patricia Akester, "Survey of technological measures for protection of copyright" *Entertainment Law Review 2001*, 12(1), p. 36-39
  - Philippe Andrieu "Les mesures techniques de protection" *Encyclopédie Juridique des Biens Informatiques* http://encyclo.erid.net/document.php?id=318#ftn14

- Valérie-Laure Benabou (Professor, University of Versailles - DANTE Laboratory) "Les routes vertigineuses de la copie privée au pays des protections techniques… A propos de l'arrêt *Mulholland Dr*ive" http://www.juriscom.net/documents/da20050530.pdf

- Tom Braithwaite "France approves law to challenge Apple" *Financial Times* (Mar 21, 2006) http://search.ft.com/ftArticle?startDate=27%2F02%2F2006&dsz=1&dse=true&queryText=apple&endDate=02%2F04%2F2006&activeTab=ftNews&aje=false&resultsToReturn=10&id=060321009950

- Nora Braun, "The interface between the protection of technological measures and the exercise of exceptions to copyright and related rights: comparing the situation in the United States and the European community" *European Intellectual Property Review 2003*, 25(11), p.496-503

- Lee A. Bygrave, "the technologisation of copyright: implications for privacy and related interests" *European Intellectual Property Review 2002*, 24(2), p.51-57.

- Christophe Caron, "Brèves observations sur la protection des mesures techniques par le droit civil*" Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/pres_caron.doc

- Charles Clark, "The answer to the machine is in the machine", *The Future of Copyright in a Digital Environment* (P. Bernt Hugenhotltz, ed., 1996), p. 139- 146.

- Nigel Davies "The digital music revolution – How will traditional rights operate in the on-line music world" *Entertainment Law Review 2005*, 16(6), p.137-143

- Severine Dusollier, "Technology as an imperative for regulating copyright: from the public exploitation to the private use of the work" *European Intellectual Property Review 2005*, 27(6), p. 201-204

- Severine Dusollier, "Electrifying the fence: the legal protection of technological measures for protecting copyright" *European Intellectual Property Review 1999*, 21(6), p.285-297

- Brian Fitzgerald and Jason Reid "Digital Rights Management (DRM): Managing Digital Rights for Open Access" (2005) http://eprints.qut.edu.au/archive/00001544/01/DRMOpenAccess.pdf

- Terese Foged, "US v EU anti-circumvention legislation: preserving the public's privileges in the digital age", *European Intellectual Property Review 2002*, 24(11), p.525-542

- Christophe Gauthier "Sans DRM, mais pas sans restrictions" *L'ordinateur individuel* (n°196 July-August 2007 p.14)

- Christophe Geiger, “Copyright and free access to information: for a fair balance of interest in a globalised world” *European Intellectual Property Review 2006*, 28(7), p.366-373

- Michael Geist “Legal fallout from Sony’s CD woes” *BBC news* (3 January 2006) http://news.bbc.co.uk/2/hi/technology/4577536.stm

- Jane C. Ginsburg “From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law” *Journal of the Copyright Society of the USA* (Vol. 50, 2003) p. 113-130 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493

- Paul Goldstein. "Copyright and Its Substitutes" *Wisconsin. Law. Review* 1997 p. 865-871

- Robin D. Gross “Digital Millennium Dark Ages- New Copyright Law Used to Threaten Scientific Research” (Nov. 7, 2001) - Electronic Frontier Foundation (EFF) http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011107_eff_felten_article.html

- F.W.Grossheide “Copyright Law from a User Perspective" *European Intellectual Property review 2001*, p. 323.

- Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan (Trusted Systems Laboratory - HP Laboratories Cambridge), “If Piracy is the Problem, Is DRM the Answer?” HPL-2003-110 (May 27th , 2003) http://www.hpl.hp.com/techreports/2003/HPL-2003-110.pdf

- Michael Hart and Steve Holmes “Implementation of the copyright directive in the United Kingdom” *European Intellectual Property Review 2004*, 26(6), p.254-257

- Michael Hart, “The copyright in the information society directive: an overview” *European Intellectual Property Review 2002*, 24(2), p.58-64

- High Level Group on Digital Rights Management, *Final Report* (March-July 2004) http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/040709_hlg_drm_2nd_meeting_final_report.pdf

- P. Bernt Hugenholtz (reviewed by Simon Stokes), “Copyright and electronic commerce: legal aspects of electronic copyright management” *Computer and Telecommunications Law Review 2002*, 8(2), p.52

- P. Bernt Hugenholtz, “Why the copyright directive is unimportant, and possibly invalid” *European Intellectual Property Review 2000*, 22(11), p.499-505

- Jean Philippe Hugot and Olivier Hugot “The DADVSI code: remodelling French copyright law for the information society” *Entertainment Law Review 2006*, 17(5), p.139-144

- Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. (New York, NY: 1990)

- International Federation of the Phonographic Industry (IFPI) *Digital Music Report* (January 2007) http://www.ifpi.org/content/library/digital-music-report-2007.pdf

- Steve Jobs "Thoughts about music" (February 6, 2007) http://www.apple.com/hotnews/thoughtsonmusic/

- Nicolas Jondet "La France v. Apple: who's the dadvsi in DRMs?" *SCRIPT-ed* (Volume 3, Issue 4, June 2006) p.7-8 http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/jondet.asp

- Ketola (Afterdawn) "CSS protection used in DVDs "ineffective" Finnish court rules" (25 May 2007) http://www.afterdawn.com/news/archive/9849.cfm

- Kamiel J. Koelman, "A hard nut to crack: the protection of technological measures", European *Intellectual Property Review 2000*, 22(6), p.272-288

- Florian Koempel "Digital Rights Management" *Computer and Telecommunications Law Review 2005*, 11(8), p.239-242

- Martin Kretschmer, "Digital copyright: the end of an era" *European Intellectual Property Review 2003*, 25(8), p.333-341

- Bernard Lamon "Affaire '*Mulholland Drive*': la copie privée sérieusement limitée" *Journal du net* (2 March 2006) http://www.journaldunet.com/juridique/juridique060303.shtml

- Lawrence Lessig *Code* – Version 2.0 (Basic books 2006) http://pdf.codev2.cc/Lessig-Codev2.pdf

- Lawrence Lessig *Free culture: how big media uses technology and the law to lock down culture and control creativity* (2004) http://www.free-culture.cc/freeculture.pdf

- Nicola Lucchi "Intellectual Property Rights in Digital Media: A Comparative Analysis of Legal Protection, Technological Measures and New Business Models under E.U. and U.S. Law" *ExpressO Preprint Series* (2005, Paper 615) http://law.bepress.com/expresso/eps/615

- Nicklas Lundblad "Is The Answer to the Machine Really in the Machine? - Technical copyright protection and file-sharing communities" http://www.skriver.nu/esociety/archives/ifip_2002_lundblad.PDF

- Colin Nasir "Taming the beast of file-sharing – Legal and technological solutions to the problem of copyright infringement over the Internet: part 2" *Entertainment Law Review 2005*, 16(4), p.82-88

- Laurier Yvon Ngombe “Technical measures of protection versus copyright for private use: is the French saga over?” *European Intellectual Property Review 2007*, 29(2), p.61-65

- Helen Padley, “Copyright – games – copy circumvention device (case comment)” *Entertainment Law Review 2005*, 16(1), N9

- Parliamentary Office of Science and Technology “Copyright and the Internet” *Postnote*, October 2002 (Number 185)

- Michael D Pendleton “The Digital Divide - International Enforcement of Digital Lockup” *Journal of Information, Law & Technology 2006* (1) Special Issue http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2006_1/pendleton/#a44

- B. Posner, “Purposes and scope of the Green Paper on Copyright and the Challenge of Technology", in *Copyright and the European Community: The Green Paper on Copyright and the Challenge of New Technology* (F. Gotzen ed., 1989), p.2-8

- Joel R. Reidenberg “ Lex Informatica: The Formulation of Information Policy Rules Through Technology” *Texas Law Review* (Volume 76, Number 3, February 1998) p. 553-584 http://reidenberg.home.sprynet.com/lex_informatica.pdf

- Tomasz Rychlicki “An opinion on legal regulations on reverse engineering and technological protections measures” *Computer and Telecommunications Law Review 2007*, 13(3), p.94-99

- Alexandra Sims, “The public interest defence in copyright law: myth or reality”, *European Intellectual Property Review 2006*, 28(6), p.335-343

- Tony Smith “Tiny C code bests seven-line DVD decoder” *The Register* (13 March 2001) http://www.theregister.co.uk/2001/03/13/tiny_c_code_bests_sevenline/

- Barry B. Sookman “Technological protection measures (TPMS) and copyright protection: the case for TPMS” *Computer and Telecommunications Law Review 2005*, 11(5), p.143-159

- Catherine Stromdale “The problems with DRM” *Entertainment Law Review 2006*, 17(1), p.1-6

- Randall Stross “Digital Domain: Want an iPhone? Beware the iHandcuffs” *New York Times* January 14, 2007 http://www.nytimes.com/2007/01/14/business/yourmoney/14digi.html?ex=1326430800&en=2c5efe51f9d74dd8&ei=5090

- Isabelle Vaillant “Le contournement des mesures techniques de protection, contrefaçon ou criminalité informatique ?” (June 2003) http://eucd.info/documents/transposition-eucd-2003-06-20.pdf

- Mikko Valimaki and Ville Oksanen "DRM interoperability and Intellectual Property policy in Europe" *European Intellectual Property Review 2006*, 28(11), p.562-568

- Adam Webb "It's the last rites for DRM…" *Music Week* (10 February 2007) p.9-10

- Jacques de Werra "The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)" *Presentation for the ALAI congress : Adjuncts and Alternatives to Copyright* (New-York 13-17 June 2001) http://www.alai-usa.org/2001_conference/Reports/dewerra.doc

- Henning Wiese, "The justification of the copyright system in the digital age" *European Intellectual Property Review 2002*, 24 (8), p.387-396

- **Legislation and official documents**

- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights *Official Journal* L 157, 30.4.2004, p. 45–86

- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167 , 22/06/2001 p. 10 – 19

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal* L 178,17.7.2000, p. 1–16

- Directive 98/84 E.C. of the European Parliament and the Council on the legal protection of services based on, or consisting of, conditional access, *Official Journal* L320, November 11, 1998 p. 54-57

- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077 , 27/03/1996 p. 20 -28

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal* L 281, 23.11.1995, p. 31–50

- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17.5.1991, p. 42–46

- COM/2004/0261 final - 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/1996/0568 – Commission communication -Follow-up to the Green paper on copyright and related rights in the information society

- COM/1995/0382 - Green Paper - Copyright and Related Rights in the Information Society

- COM/1988/0172 - Green Paper on copyright and the challenge of technology - Copyright issues requiring immediate action

- Loi n° 2006-961 1st August 2006 "relative au droit d'auteur et aux droits voisins dans la société de l'information" *Official Journal* 3rd August 2006

- articles 323-1 to 323-7 of the French criminal code

- The Copyright and Related Rights Regulations - Statutory Instrument 2003 No. 2498, 31 October 2003 (amending the Copyright, Designs and Patents Act of 1988) http://www.opsi.gov.uk/si/si2003/20032498.htm

- The Copyright, Designs and Patents Act 1988 (c. 48) http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

- The Computer Misuse Act 1990 (c. 18) http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

- The Digital Millennium Copyright Act (1998) http://thomas.loc.gov/cgi-bin/query/F?c105:6:./temp/~c105TjnYFD:e884:

- *The United States Code* Title 17 "Copyright Law of the United States of America and Related Laws" Chapter 10 "Digital Audio Recording Devices and Media" § 1002. http://www.copyright.gov/title17/92chap10.html#1002

- WIPO copyright treaty, 20 December 1996 http://www.wipo.int/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf

- Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, revised at Paris on July 24, 1971, and amended on September 28, 1979

- European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") of 4 November 1950

- **Cases**

  - *Sony Computer Entertainment UK Ltd v Gaynor David Ball & 6 Ors* [2004] EWHC 1738 (Ch)

  - TGI Paris (3° ch., 2° sec.) 30 April 2004 – Cour d'appel de Paris (4° ch.) 22 April 2005 - Cour de cassation (1° ch.), 28 February 2006, *s.a. Studio Canal, s.a.s. Universal Pictures Vidéo France et Syndicat de l'édition vidéo c. M. Perquin et association U.F.C.-Que choisir*.

  - Cour d'appel de Paris (4° ch. section A) 4 April 2007 *UFC Que Choisir, M. Perquin c. Films Alain Sarde and others*

  - Conseil de la Concurrence *"Décision N° 04-D-54 relative à des pratiques mises en oeuvre par la société Apple Computer, Inc. dans les secteurs du téléchargement de musique sur Internet et des baladeurs numériques*" november 9, 2004

  - *Sony Corp. of America v. Universal Studios Inc.*, 464 U.S. 417 (1984),

  - *Felten v. Recording Industry Assoc. of America*, 6 June 2001, U.S. District Court for the District of New Jersey, Case no. 01 CV 2669

  - Helsinki District Court Judgment 07/4535 - 4/10 Dept. 25 May 2007 R 07/1004 http://www.turre.com/css_helsinki_district_court.pdf

  - *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* - ECJ, Case C-418/01, April 29, 2004

  - *Radio Telefis Eireann ("RTE") and Independent Television Publications Ltd ("ITP") v Commission of the European Communities*, ECJ, Joined Cases C-241/91 P and C-242/91 P, April 6, 1995

  - *Silver v. United Kingdom*, 25 March 1983, Series A, No. 61, (1983) 5 EHRR 347

- **Online databases and websites**

  - EBSCOhost

  - Eurlex

- Journal of Information, Law & Technology (JILT)
- Juriscom.net - droit des technologies de l'information
- JSTOR: Basic Search
- Westlaw.com

- ALAI 2001 Congress
- Apple website
- BPI file-sharing factsheet
- Campaign for Digital Rights - FAQ
- Chipping away the infringers? : The Journal Magazine : The Journal of the Law Society of Scotland
- Creative Commons
- Digital Rights Management (DRM) Architectures
- ECMS: legal issues
- ECMS: technological issues
- EFF: Digital Rights Management and Copy Protection Schemes
- EMI music copy control
- EUCD-info
- Europa-SCADplus
- Euro CopyRights - The Protection of Technological Measures in Europe (EUCD) - Can I copy a CD or DVD? - Home > France > Explanatory memoranda
- Fritz Machlup biography
- IFPI
- Internal Market - COPYRIGHT AND NEIGHBOURING RIGHTS –
- ISRC
- ISWC

- Sky hit by Windows Media DRM crack | CNET News.com
- SPPF: Right's protection
- The Register
- wikipedia