E

WIPO

WCT-WPPT/IMP/2
ORIGINAL: French
DATE: November 23, 1999

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

# WORKSHOP ON IMPLEMENTATION ISSUES OF THE WIPO COPYRIGHT TREATY (WCT) AND THE WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT)

## Geneva, December 6 and 7, 1999

LEGAL PROTECTION OF TECHNOLOGICAL SYSTEMS

*presented by Alain Strowel*
*and Séverine Dussolier*

CONTENTS

Introduction and scope

In December 1996, the international community negotiated and adopted two major treaties within the World Intellectual Property Organization, designed principally to adapt the legal framework of copyright and related rights to new technology.[1] Two provisions in these treaties have instituted a new form of protection concerning technological measures which protect works. Many States have already transposed these particular points into their national law; others are in the process of doing so.

The purpose of the present study is to make a comparative analysis of these different national or regional measures, their scope and the way in which they are implemented, and also to present other texts which establish similar protection for technological measures.

Particular attention will be paid to the question of the interaction of limitations of copyright and legal protection for such technologies, as well as the definition of those elements which are necessary for adequate and effective protection in the case of their circumvention.

## A. TYPOLOGY OF TECHNOLOGICAL PROTECTION MEASURES

New technologies which are liable to be used by authors and other rightholders to protect their works and other services[2] within the information society are extremely diverse. Some have been specifically designed to counter the threat that digital progress poses to copyright, others have been developed in order to protect all types of digital content, regardless of whether it is copyrighted or not.

It is difficult to draw up an accurate list of technological measures in existence or which are being developed, just as it is impossible to predict the future of such technologies in the domain of protecting works under copyright.[3]

We have therefore chosen to present and to group the technological measures relating to protection of copyright and related rights under four categories, according to the principal aim of the measures. In this way measures which effectively protect an act under copyright can be defined, as can systems of conditional access, marking and identification tools and systems of electronic rights management. In each category clear examples of technologies will be succinctly presented.

---

1 J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI: *The New WIPO Treaties: a First Résumé*, *European Intellectual Property Review (E.I.P.R.)*, 1997/4, P. 173; A. LUCAS, Droit d'auteur et numérique, Droit@Litec, 1998, p. 270 and onwards.

2 Hereinafter, for ease of reference, we shall speak only of protection of copyright on works, without necessarily mentioning protection of related rights with regard to a range of content and services.

3 D. GERVAIS, *Electronic Rights Management and Digital Identifier Systems*, Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, First Session, Geneva, 14 and 15 December 1998.

## 1. Technological measures which protect copyright

This relates to technical tools which prevent any acts being carried out or use being made to which the rightholders hold exclusive rights, such as printing, communication to the public, digital copying, alteration of the work, etc. Reference is made notably to anti-copy systems where the main aim is to prevent copies of the work or of the protected object being made, either in digital form only, or in both digital and analog form. For example, the **dongle**, which is principally used in the software sector, usually consists of one piece of hardware,[4] a type of key, which can be connected to the serial port in the computer. Any program protected by this system can be connected to the key to check the scope of the user's rights. The principle of the dongle appears to have been a precursor of **smart card technology** which enables a greater amount of information to be stored. Furthermore these smart cards can contain pre-paid units. In contrast to dongles, where the use is thus far limited to expensive software programs, smart cards will doubtless be more frequently used for software and for other works available to the general public. These two forms of technology are aimed both at access and control of use, particularly in relation to copying.

The **Serial Copy Management System** is a system primarily used in the United States on audio digital taping devices such as DATs and mini-disks. This technology enables the machine to decrypt audio signals which are embedded in the input medium and specifically to decrypt the data relating to its protection. The system authorizes one single digital copy to be made from the original but does not permit any further copying. A similar system, the **Content Scrambling System**,[5] which is based on the cryptography technique has been placed on DVDs in order to prevent all copying.

## 2. Access systems

One of the major challenges facing digital networks is to make access to information and to protected content secure, both in order to ensure payment of a fee and to protect copyright to the work which has been "padlocked" in this way. Many systems have therefore been designed in order to guarantee and make access secure, whether it be to a work, or group of works, or to a service which specifically includes protected works. Deactivating the mechanism which monitors access can be done either through payment or once other conditions of the licence agreed to with the rightholders have been met. The access mechanism can either control initial access and then leave the work free for any further use or a check can be made that conditions have been met each time access is requested. Access can also be differentiated with ease according to the type of user, and this is the huge advantage of these systems. For example, a university may have obtained access by paying an annual fee for a work or a collection of works, for a certain number of students or for one year. The system will check in such cases for a decrypting key on the university's computers or for a password agreed by contract, or even via the student's identity. Conversely, the same technology can provide repeated access to an individual in exchange for a renewable payment, usually proportionate to the frequency of use.

---

4 A diskette can also be inserted by the user when he/she wishes to use a computer program. The program will only work if the diskette is inserted.

5 D. MCCULLOUGH, *Blame US Regs for DVD Hack, Wired News*, 11 November 1999.

There are numerous technologies which can do this: cryptography, password set-top boxes, black-boxes, digital signatures, digital envelope.[6] The **cryptographic** procedure is well-known. It can be defined, as in the French law governing telecommunication, as "*transformation through secret conventions of information or clear signals in data or unintelligible signals for third parties, or to carry out the opposite operation through means designed to this effect*".[7] In the digital world, encrypting and decrypting is carried out through algorithms of varying degrees of complexity. **Digital signatures** are a particular application of encrypting carried out to certify and identify a document.[8] Within the context of protection of copyright this technology is principally used to secure transmissions of works over networks and to prevent access to the work by any unauthorized person. Provision of a decrypting key is made through payment of a fee or by meeting other conditions on which use of the work is dependent.

**Digital envelope** or **digital container** is an application of cryptography through which a work is "inserted" into a digital envelope containing the information relating to the product and the conditions of use of the product. It is only by meeting the conditions (such as payment of a fee, using a password, etc.) that the envelope can be opened and the user is granted access.

## 3. Marking and tattooing tools

Several techniques are able to play an identification rôle and to mark products.[9] The objectives of the techniques are varied: the principle is to serve as a visible or invisible means for inserting data relating to the work, whether it be the title of the work, the identity of its creator and the rightholder, or conditions of use. This rôle is specifically protected under article 12 of the WIPO Treaty on copyright, which relates to the protection of information in the domain of rights. We are referring here mostly to **watermarking** or *tatooing* which means certain information can be inserted as a watermark within the product's digital code. Such watermarking is generally invisible and inaudible. The invisible inscription is made through the steganography technique, which can be defined as "*the art and science of communicating in a way which hides the very existence of such communication*".[10] Invisible ink is an example of this millennium science borrowed from the analog world. In a digital environment watermarking modifies certain so-called "useless" bytes of an image or a sound.[11] By means of an appropriate computer program the digital code can be extracted and

---

6 Dongles and smart cards (see above) can also be used to control access.

7 Law 90-1170 of 29 December 1990, O.J., 30 December 1990, p. 16439.

8 J. HUBIN, Y. POULLET, with the collaboration of B. LEJEUNE and P. VAN HOUTTE, *La Sécurité informatique, entre technique et droit*, CRID Notebook nº 14, Brussels, Story-Scientia, 1998.

9 S. DUSSOLIER, *Le droit d'auteur et son empreinte digitale, Ubiquité*, nº 2, May 1999, pp. 31-47.

10 R. LEYMONERIE, *Cryptage et Droit d'auteur, Les Cahiers de la Propriété Intellectuelle*, 1998, Vol. 10, nº 2, p. 423; also see D. GUINIER, *La stéganographie, De l'invisibilité des communications digitales à la protection du patrimoine multimédia, Expertises*, June 1998, pp. 186-190.

11 These bytes are useless in the sense that images and sounds include a large number of bytes which, if eliminated or modified have no perceivable consequence for the listener or spectator. For example, in the case of a phonogram, the line of the digital code allowing marking is inserted into the bytes containing frequencies the human ear cannot hear.

decoded. Watermarking is generally indelible and can be found in every part of the work, even where it has been altered or cut up.

However, other features of these technologies allow more or less direct protection of copyright. Firstly watermarking is in some cases entirely visible, a "stamp" is in these cases clearly placed on the representation of the product, in a way which is somewhat similar to the placing of the word "SPECIMEN" on samples of banknotes or of other official documents. This practice, also known as "**fingerprinting**", is quite widely used in photographic agencies which put their name or logo on photoprints with the sole aim of advertising and do not provide the picture without such additions until payment of the agreed-upon fee has been made. It is also the case in some on-line museums or archives where reproductions in the collections carry the museum's stamp.[12] The visible watermarking in this case fulfils the purpose of protecting the product against copying since the mark which is clearly visible represents a decrease in value on something which is freely accessible through the networks.

Each different copy of the work distributed to users can furthermore include a particular digital serial number. In this way a pirate copy discovered later on the market can reveal the original copy from which the counterfeit has been made. Stamping every copy in this way will make it possible to find the origin of unauthorized copies of the original copy by means of a database containing all users and serial numbers to whom the stamped specimens have been licensed. Here the principal aim of the protection technique is to provide proof in terms of counterfeit. A final useful function of watermarking is to authenticate the content, namely by ensuring that it remains intact.

## 4. Electronic management systems

Electronic management tools are all those technologies which ensure management of rights on networks by allowing the issue of on-line user licenses and by monitoring the use of works. Other functions can also be overseen by these methods: distribution of rights, collection of payments, sending out invoices, carrying out data gathering on the profile of users, etc. As an example, **electronic agents** have recently appeared on the market.[13] Developed to carry out numerous functions on the networks, some of them are programmed to negotiate and to enter into electronic contracts.[14] This technology is also beginning to be applied to copyright where the contracting agents accompany the dissemination of the protected content on the Internet both to show terms and conditions of user permits and to receive and manage acceptance or the click of a user's mouse. Other more sophisticated agents manage distribution and the use of the product in a completely automated manner, in particular by integrating an electronic payment system, renewing users' permits or by making a precise calculation of use (for example, analyzing which works have been copied, printed, enlarged or downloaded and how many times), both in order to have accurate accounts

---

12 An example of this is the Vatican Library where precious documents have been digitized and made available on-line to the public, however, they bear the Vatican's seal which prevents any form of commercial use of them.

13 R. JULIA-BARCELO, *Electronic Contracts = A new legal framework for electronic contracts: the EU electronic commerce proposal*, *Computer Law and Security Report (CLSR)*, 06/1999, nº 15/3, pp. 147-158.

14 S. GAUTHRON AND F. NATHAN, *On-line services and data protection and the protection of privacy*, Study carried out for the European Commission, DG XV, p. 31.

reflecting real use and for marketing purposes at a later date (identifying which user likes which type of music, for example). Distributing rights destined for authors and performing artists as well as for other rightholders could conceivably be made on-line by such agents. Where these agents are limited to controlling the use of products and drawing up a list of the number of times the products and web sites are consulted in order to identify precise profiles of users, they are often referred to as **metering systems**.

**Electronic Right Management Systems** or **ERMS** are undoubtedly protection measures which are the most often referred to, although one must take care not to view them as one specific technology. The **ERMS** (also known as **ECMS** for the **Electronic Copyright Mangement Systems**) consist rather of a combination of several tools and technologies aiming to carry out several functions.[15] A cryptographic tool which blocks access to the product can be linked to an anti-copy system which prevents a work from being copied even by a legitimate user. The **watermarking** technique (see above) and an electronic licensing and payment system can also be integrated into the same computer program. Usually the main aim of ERMS is to manage use and licenses for on-line works. This is why we have placed them within the category of management tools.

Furthermore, technologies being developed at the moment and which copyright holders are likely to subscribe to in order to protect their works have many more marginal functions which in some cases lie far outside the strict bounds of intellectual property itself. These are principally:

- setting out of terms and conditions for use of the product;
- secure transmission of the product
- proof of receipt of the content and the identity of the person who has legitimately received this content;
- payment;
- recording and following up on use, particularly with a view to charging appropriately or for marketing.

These roles are essential for the supervision and remuneration of copyright holders. However, technologies which ensure the smooth running of other aspects to the transaction between an author and a user will not necessarily be covered by legal texts protecting technological measures. Another legal basis must therefore be found to prosecute potential counterfeiters of the complementary systems. This issue goes beyond the scope of the present study.

---

15 M. LEDGER AND J.P. TRIAILLE, *Dispositions contre le contournement des dispositifs techniques de protection*, in *Copyright in Cyberspace*, ALAI Study Days, Amsterdam, June 1996, Ed. ALAI, 1997.< http://www.droit.fundp.ac.be/espacedroit/textes>; D. GERVAIS, *Electronic Right Management Systems (ERMS), The next logical step in the evolution of rights management*, (1997), see http://www.copyright.com/stuff/ecms_network.htm.

## B. LEGAL MEASURES FOR THE PROTECTION OF TECHNOLOGICAL SYSTEMS

We have seen how the technology which authors and other rightholders use to protect their products usually has different functions and is likely to ensure security and electronically manage a vast amount of content and digital information which perhaps is not protected by an intellectual right. The same system of monitoring access can be used for web sites which contain music, uncomplicated financial information or for broadcasting television programs on the Internet. The consequences are multiplied.

On the one hand, technologies are and will be used by different operators for different reasons. Consequently legal protection for such technologies may be sanctioned by other legal texts rather than those relating to intellectual property.

On the other hand, circumvention systems and mechanisms to circumvent these technologies which appear on the market to circumvent a type of technology, can be used indiscriminately for a number of different objectives. The primary goal of these illicit measures is, therefore, not necessarily to prejudice content protected by copyright or related rights, thus the legal arsenal should make provision for sanctions outside the narrow context of intellectual property. For example, a hacker can try to demolish a protective measure relating specifically to content protected by copyright (as in the case, for example of the persons who have recently revealed on the Internet how to circumvent the DVDs anti-copy protection), but s/he can also develop a means of circumventing a security measure, which could then be used with the aim of violating copyright. In order to prevent such measures, rightholders may refer to legal texts other than those which transpose the WIPO Treaties into national law.

This is why, after having studied the legal measures which specifically protect intellectual rights (item 1), in comparative law, we propose to give an idea of other legal measures which could sanction circumventing technology which protects copyright, such as the European Directive on the legal protection of services based on, or consisting of, conditional access (item 2), or other national measures in terms of criminal conduct in the computing industry (item 3).

### 1. Protection relating specifically to intellectual property

#### 1.1. Criteria for comparison of legal measures

During the 1996 Diplomatic Conference member countries of WIPO were unable to agree on a very detailed set of rules for safeguarding technological measures which protect copyright and related rights. The text of the Treaty calls upon States to adopt legal protection "*against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights … and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.*" Article 11 of the WIPO Treaty on copyright and article 18 of the Treaty on Phonograms does not give any detail as to how such protection should be organized,[16] nor which are the specific acts which should be prohibited. Complete freedom is given to States on this point, which means that national measures are liable not to be in line with each other, even if they appear on

[16] J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI, *op.cit.*, p. 173.

examination to be inspired by the European and American models.

Many countries have begun or completed the transposition of obligations relating to legal protection of technological measures which are the outcome of the 1996 WIPO Treaty, into national law. The complexity of these new national measures and of these projects is vast. We shall analyze legal measures which have already been adopted according to various criteria which are:

- **The aim of the protection and definition of technological measures**: not all technological measures are necessarily protected in all of the texts. Where the WIPO Treaty speaks in general of "*effective technological measures that are used by authors in connection with the exercise of their rights*", national measures are usually more precise and limit protection by defining either the technological measures concerned, or the criterion for efficiency which would justify such protection. We will also see that legislators have often instituted a dual protection both for systems which control access to products and for systems which directly protect exclusive copyright.

- **The scope of the prohibition (an act of circumvention and/or acts preparatory to circumvention):** WIPO texts appear to concern only the act of circumvention of the technological protection measure itself. However, copyright holders and legislators stress the need for forbidding so-called acts preparatory to circumvention, which the manufacture of circumvention devices and making them available to the public represent. It is, in fact, clear that the prejudice caused to rightholders will be even greater if the technical means for circumvention are easily and widely available on the market. From that point, most measures or national projects bring a twofold charge, firstly, with regard to persons who have circumvented the technological measure and secondly with regard to the marketing of devices which are likely to allow or to facilitate such circumvention.

- **Type of illicit preparatory acts**: in general, legislators are strict in determining activities which are entail the responsibility of manufacturers of circumvention devices. In such cases illicit activities are listed, passing from manufacture to all kinds of distribution to the public of illicit devices. In this context we shall examine whether those that provide circumvention services are also incriminated.

- **Conditions relating to the illicitness of devices**: one fundamental question is to determine at which point a seemingly lawful device can be considered to be illicit. A large number of electronic or computing devices are specifically designed to circumvent the technological measure and are explicitly marketed with this aim. Others can be diverted from their original legitimate function in order to serve a more illicit purpose. Therefore it is essential to clearly define the line between lawful devices and those which are not.[17] A clear and precise definition of illicitness is, moreover, a major concern within the electronic equipment industry which calls for some security from a legal point of view. Let us take, for example, a video recorder which is to be used primarily for watching and recording audiovisual progams but which also has a secondary capability which is

[17] Th. VINJE, *A brave new world of technical protection systems: Will there still be room for copyright?, EIPR*, 1996, nº 8, p. 431.

to circumvent technical protection which has been placed on video cassettes. Is the video recorder illegal? What is the position for an encrypting software program which is used mostly to decrypt certain signals without authorization? To sum up, the question is whether it is enough for the circumvention function to exist, albeit as a secondary function, or whether it must be the chief or over-riding aspect of the device or program.

- **Knowledge of the infringement in terms of responsibility:** Some legal texts require that the perpetrator of illegitimate acts have some knowledge of the infringement of copyright law. In some legal systems the perpetrator of a circumvention act will only be held responsible if s/he knew or should have known that in so doing s/he was infringing copyright.

- **The situation with regard to copyright limitations**: one of the most controversial questions in the area of legal protection of technological measures is that relating to limitations of and exceptions to copyright and particularly the question of knowing whether it is admissible to circumvent technological protection to carry out an act which has not been authorized by the author. This question of exceptions has two facets, in fact. Firstly, where circumvention of technological measures controlling access and the use of a work which has come into the public domain takes place, or where use is exempted because of a legal exception, should circumvention be tolerated? Or should one consider the manufacturing and marketing of circumvention systems which are designed simply to cancel technologies added to components in the public domain or which allow the exercise of a right to exemption as unlawful.

- **The existence of exceptions to the ban on circumvention**: in some cases legal protection of technological systems is accompanied by a series of exceptions. Here the act of circumvention and/or manufacturing or distributing illicit devices eschews the principle of prohibition.

- **The existence of a no mandate clause**: some systems require recognition by the reading, downloading or copying device. Protection here is integrated into the input medium or in the digital code of the work which sends a control flag to the device to prevent it from carrying out certain functions (copy, print, access, for example). The electronics and computing industry is concerned that it may be obliged to include in its components mechanisms which will allow interaction with these signals. The electronics industry therefore argues for a clear clause in law of a measure which would dispense them of the need to adapt their products to the technological measures. Such a measure is generally referred to as a “no mandate” clause.

1.2. Protection of technological measures within the European Union:

a) The directive on the protection of computer programs and its transposition into Member States' law.

The European legislator first examined the issue of legal protection of technological measures when the directive of 19 May 1991 on computer programs was drawn up. Article 7 (1) c requires Member States to incriminate persons who carry out 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.*"[18]

The technological measures which are protected herein are not truly defined in the European text. Only technological measures protecting computer programs are alluded to, and this in a vague manner. It could therefore be considered that, when they are applied to software, most of the systems which we have enumerated above might fall within this definition, whether they relate to protection of access or the copying of the program.

This measure does not target the act of circumvention itself, only so-called preparatory activities. In the text before us, for example, the acts of putting into circulation or possession for commercial purposes are unlawful. Putting something into circulation can be done by sale, offer to the public, renting, etc.

Devices and systems which are prohibited from being put into circulation are any means where the intended purpose is to facilitate the elimination or the circumvention of the technical measure. This criterion is both wide and yet also restrictive. Firstly the term"sole aim" seems to indicate that a whole range of mechanisms, software, elements of a system and devices are targeted. However, the criterion of "sole aim" vastly reduces the range of measures which are considered unlawful. For example, a software program which has a perfectly legitimate objective but which also happens secondarily to permit circumvention of the technical measure will not be covered by the prohibition, even if it is clear that the program's success with users is largely due to the secondary function. This criterion of sole aim means that a large number of systems are exempted from the prohibition.[19]

Germany has nonetheless interpreted this criterion very broadly,[20] the sole aim of the application and not of the program overall having been considered as sufficient to prohibit the distribution of the software program which allows circumvention. Such a broad interpretation of the text means software programs containing applications where the sole aim is circumvention may be prohibited, even if the software program also has other purposes.

In other Member States, transpositions into national law do not move away greatly from the text of the directive. For example, Germany has inserted into its law on copyright a measure which prohibits the means which aid the unauthorized removal or circumvention of technological measures protecting programs.[21] Belgian law sanctions "*those who put into circulation or possess for commercial reasons the means, the sole aim of which is to facilitate*

---

18 Directive on the legal protection of computer programs of 14 May 1991, O.J. L 122, 17.5.1991.

19 Th. VINJE, *op. cit*., p. 431.

20 A. RAUBENHEIMER, *Softwareschutz nach den Vorschriften des UWG, CR*, 1994, p. 264

21 Section 69 of *Gesetz uberUrheberrecht und verwandte Schutzrechte*.

*the unauthorized elimination or the circumvention of technological measures which protect the program*".[22]

The proposal for a European directive on copyright and related rights in the Information Society which will be presented hereinafter forecasts that the legal protection that it decrees will not affect in any way the specific measures for protection provided for by the directive on the legal protection of computer programs. Nonetheless, it would be illogical to retain this system which provides limited protection for measures where the sole aim is the circumvention of computer programs when the future directive on copyright will introduce a wider form of protection for all the other types of works.

b) Proposal for a directive on copyright and related rights in the Information Society.

Article 6 of the revised proposal for a directive on the harmonization of certain aspects of copyright and related rights in the Information Society[23] is drafted as follows:

"*1. Member States shall provide adequate legal protection against the circumvention without authority of any effective technological measures designed to protect any copyright or any rights related to copyright as provided by law or the sui generis right provided for in Chapter III of European Parliament and Council Directive 96/9/EC, [directive on databases], which the person concerned carries out in the knowledge, or with reasonable grounds to know that he or she pursues that objective.*

*2. Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices, products or components or the provision of services, carried out without authority, which:*

*a) are promoted, advertised or marketed for the purpose of circumvention of, or*

*b) have only a limited commercially significant purpose or use other than to circumvent, or*

*c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,*

*any effective technological measures designed to protect any copyright or any right related to copyright as provided by law or the sui generis right …*

---

[22] Article 10 of the Belgian Law of 30 June 1994, transposing the European Directive of 14 May 1991 into Belgian law.

[23] Amended proposal for a directive on the harmonization of certain aspects of copyright and related rights in the Information Society, COM (1999) 250 final, 21 May 1991.

*Prohibited activities*

After a detour via the European Parliament it was decided that both acts of circumvention as well as preparatory activities be incriminated in the text. The initial proposal allowed some vagueness on the item concerning "any activities". At present the article is subdivided in two separate paragraphs, one which incriminates unauthorized acts of circumvention, the other incriminating manufacturing and distribution activities relating to unauthorized devices.

*Protection aim*

Whether it is circumvention or distribution of the means for circumvention those technological measures which are protected are defined as *"any technology, device or component that, in the normal course of its operation, is designed to prevent or inhibit the infringement of any copyright or any right related to copyright (…) or sui generis right (…).* At first sight this definition would only cover measures which establish direct protection of copyright, such as anti-copy systems.

However, and in accordance with WIPO treaties, the technological measures should be effective in order to benefit from protection. The European legislative body has given a definition for this criterion of effectiveness: "*Technological measures shall be deemed "effective" where the access to or use of a protected work or other subject matter is controlled through application of an access code or any other type of protection process which achieves the protection objective in an operational and reliable manner with the authority of the rightholders. Such measures may include decryption, descrambling or other transformation of the work or other subject matter*."

This definition of the effectiveness of technological measures invites several observations. Firstly, the criteria for effectiveness are, either the fact that access to the work is controlled from a technical point of view, or that its use is. However, access to a work or to any other protected object is not in itself necessarily an act which falls under the author's exclusive copyright or the copyright of a related rightholder.

The initial text put forward by the Commission moreover limited the definition of effectiveness of access.[24] The European Parliament has caused the criterion of use to be added, which means acts carried out by the user can be covered more broadly, including acts of copying and communication to the public which should be authorized by the rightholders. This modification is related to the first paragraph which emphasizes more clearly that the protection is directed at technological measures which protect all copyright or related rights. Therefore, if under the first text it seemed as if anti-copy systems did not enjoy any protection, it now seems to us that the new definition will make it easier for them to be protected. Nonetheless, the protection which has finally been instituted is surprisingly broad because it includes all acts carried out by the user (from first access to the work to all subsequent uses). We will return to this point in the last section of this study.

Furthermore, the definition makes it clear that technological measures must have been

---

[24] S. DUSOLLIER, *Electrifying the Fence: The legal protection of technological measures for protecting copyright*, E.I.P.R., 1999, nº 21/6, p. 285-297.

applied to the work or the protected object with the agreement of the rightholders, whether they are the authors, performing artists, producers or exploiters. However, the scope of this authorization is not clear. Is the exploiter who wishes to secure distribution of the works by a technological protection system obliged to obtain authorization from all the rightholders? Let us take a media library which would like to make the media which it hires or lends secure, with the authorization of all rightholders or as provided by law. Would the library have to obtain specific authorization from each rightholder? If it does not obtain this, does that mean that the library cannot then prosecute persons who circumvent the protection? Generally speaking, does that mean that only technology used by rightholders will be protected? This could represent a rather incomplete form of protection insofar as works on some lawful distribution networks, although they might be protected technically, could be copied and used despite this protection. It should be noted that in this case, however, other legal documents may provide protection for these systems such as the directive on conditional access, although we shall see that in this case the act of circumvention will not be liable to sanction itself.

Finally, it is made clear that protection procedures include decrypting or descrambling systems[25] as well as any other transformation of the work. Transformation of the work could, in our view, include watermarking techniques or tatooing of the work which, as we saw earlier, are only an indirect means of protection for the work. These three types of procedures are, however, only cited as examples, and therefore the possibility that dongles or other systems might well be targeted also should not be excluded.

*Illicit or irresponsible types of activities*

We saw that paragraph 1 of article 6 from now on explicitly includes the very act of circumvention of technological measures in the range of illicit activities. In this case a moral element has, in fact, been added with a view to only prosecuting persons who have carried out circumvention of the technological mechanism with full knowledge of the facts. The text speaks of acts "*which the person concerned carries out in the knowledge, or with reasonable grounds to know that he or she pursues that objective [that of non-authorized circumvention]*". It is a condition of knowledge, which does not appear in the parallel offence of manufacturing circumvention devices.

In the case of preparatory activities the European text is very wide-ranging since it targets "the activities" in a rather vague manner. The manufacture of, or distribution of illicit devices or the provision of services are only cited as examples. Therefore, it would seem to us that all marketing activities of these unauthorized devices is covered. It also seems to us that non-commercial activities of supplying circumvention systems are also targeted. Thus the distribution of decrypting keys on the Internet, even if it is without a lucrative goal, as is happening at present with the decryption of the technical protection of DVDs, would also be considered to be illicit.

[25] Which clearly demonstrates that this text is principally aimed at crippling and access systems.

*Illicit devices*

The definition of unlawfulness of devices and services is for its part dependent on three alternative criteria. Either the system or the service must be the subject of a promotion campaign, of an advertisement or of a marketing campaign, with the aim of circumventing technical protection; the commercial purpose or the use of such devices is principally for circumvention. Lastly, the system or service is illicit where it is primarily designed, produced, adapted or carried out with a view to enabling or facilitating circumvention.

Services and devices which clearly have the function of circumventing technological measures pertaining to it, or those which show from their design, or from their conception or by the public image given to the product are targeted in some way, as are services and devices where the main function or use is to circumvent technological measures.

Here too, and this is quite common, the distinction between lawful and unlawful systems will remain blurred and subject to the discretion of the courts. As an example, encrypting software principally used for decrypting protected works will be forbidden. As far as video recorders are concerned, even if the circumvention function is only secondary, the fact that the product has been promoted to this end will be sufficient to render it unlawful.

*Limitations of and protection of copyright*

In the revised text of the proposal, the European Commission reiterates that technological protection must be set up with a view to safeguarding copyright or related rights and therefore within the limits of those.

Furthermore one preamble clearly states that circumvention, in order to be ruled illegal must be without the authority of the rightholders and not conferred by law. [26] This provides no ruling on the issue of circumvention acts which are carried out with the aim of exercising a right of exemption. Technological systems only prevent carrying out acts which fall under copyright (for example, copying, communication, modification of the work) indiscriminately without being able to determine if the act prevented by technological protection results from the legitimate exercise of an exemption right. The same technological measures will also indiscriminately protect works protected by copyright and those which have fallen into the public domain.

Nor does preamble number 30 rule that circumvention is legal if it is carried out in accordance with an exemption. The text should state in detail that the act of copying or use post circumvention must have been authorized by the author or conferred by law.

Only private copying is clearly covered, both in article 5, paragraph 2, b) bis, which authorizes private digital copying only where there is an absence of technological measures to prevent it, and in preamble number 27 which adds to this first principle that the exemption in terms of private copying cannot justify an unauthorized act of circumvention. Consequently, circumventing an anti-copy protection in order to make a private copy of a work will be forbidden.

---

[26] Preamble 30, *in fine*.

The fact that the Commission has not, on this point, followed the amendments the Parliament proposed, namely, to apply this solution to all exceptions, may indicate that in the present state of the text other exceptions are not removed by technological protection measures, indeed that their circumvention would be authorized in this context.

Even though the Commission states in its report on its motives that this question in the report regarding exceptions is regulated by the text of article 6 itself on technological measures, particularly through the definition of these, which necessitates a violation of copyright, the question is far from being resolved definitively.

*Exceptions to the ban on circumvention*

In contrast to the American text, the draft proposal for a directive does not list a series of exceptions to the ban on the principle of circumvention. The preambles in the directive inform us that protection established in this way will not be able to present an obstacle to research on cryptography, [27] nor to decompilation of software packages authorized by the directive issued in 1991 on the matter.[28] Acts to circumvent technological measures in order to test the effectiveness of the encrypting algorithm will remain permitted, as well as over-riding a protection mechanism order to decompile the software package. In this last case, however, the decompilation must take place within the strict conditions set out by the directive on the protection of computer programs, particularly in that the person must be a legitimate user of the program and provided that information necessary for interoperability is not available in any other manner. Thus the decompilation can only be carried out (and this also applies to the circumvention of the technological measure in order to do so) with the sole aim of achieving the inter-operability of the program.

*"No mandate" clause*

Subsequent to discussions held in the European Parliament, the revised proposal now includes a no mandate clause amongst its preambles. Thus in preamble 30 bis it is written that protection cannot prevent "*the normal operation of electronic equipment and its technological development; whereas such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures*". The main objective for the Commission here is to encourage negotiations between rightholders and the electronics industry in order to achieve integration of technological measures in electronic and computing equipment.

---

27 Preamble 30 bis, *in fine.*

28 Preamble 31, *in fine.*

1.3. Protection of technological measures in the United States:

a) Section 1002 of the Copyright Act: protection of Serial Copy Management Systems

When tools which enabled recording and copying of audio digital data files first began, commonly known as **Digital Audio Tape** or, the American disk industry and rightholders were excited to note that such systems **DATs** could permit large-scale copying of musical works without any loss of quality and at a lower cost.

A modification of the Copyright Act was then adopted to impose the insertion within DATs of an anti-copy mechanism which would prevent carrying out more than one digital copy of a work (through Serial Copy Management Systems). In that case, the industry was obliged to make its production conform to the technological systems available at that time, and therefore, it was a measure which did not respect a "no mandate" clause.

This legislative modification also includes a ban on importing, manufacturing, distributing, supplying or lending a service where the primary effect or aim is to circumvent the anti-copy technological measure.[29] It is useful to note that in a recent ruling, [30] an American judge considered that these measures were to be strictly interpreted and could not therefore be extended to other systems than the DATs. The phonographic industry tried to force manufacturers of MP3 data file readers such as the Diamond firm, to insert a system in their equipment to prevent copies of data files being made as well as preventing the reading of pirate data files.

b) Digital Millennium Copyright Act

In October 1998 the American Congress passed the **Digital Millennium Copyright Act**, a long legislative text which revised the **Copyright Act**. Designed both to transpose WIPO treaties and to carry out certain items on the American digital agenda,[31] this legislative reform deals with protection of technological measures.

The new section 1201 of the American Copyright Act holds that:

*(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES*

*(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter (…)*

*(2) No person shall manufacture, import, offer to the public, provide, or*

---

29 Section 1002 (c) "No person shall import, manufacture, or distribute any device, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system described in subsection (a)."

30 RIAA v. Diamond Multimedia Systems, Inc., No 98-56727 (9th Cir., June 1999).

31 J. GINSBURG, *Chronique des États-Unis, R.I.D.A.*, January 1999, p. 147 and onwards.

*otherwise traffic in any technology, product, service, device, component, or part thereof, that:*

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

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

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

*(b) ADDITIONAL VIOLATIONS*

*(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that:*

*(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;*

*(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or*

*(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.*

A dual protection is thus established, one relating to technological systems which control access to protected works, the other with regard to technological measures which effectively protect exclusive copyright. In reality three offences are instituted by the American text: (1) the *circumvention of technological measures* of protection which *control access* to protected works; (2) *the manufacture and circulation* of measures, of devices or *offering services* enabling the circumvention of systems *controlling access*; and finally, (3) the *manufacture and dissemination* of means or offering services which would permit the circumvention of *technological measures for protection of copyrights*. These three aspects warrant separate examination.

(i) Protection of systems controlling access

*Protection aim*

The technological measures targeted are those which "*if the measure, in the ordinary course of its operation, requires the application of information, of a process or a treatment, with the authority of the copyright holder, to gain access to the work.*" This certainly includes encrypting, digital envelope, dongle and key words.

The aim and main function of technologies being discussed is to control access to a work, not to an example or a copy of the work.[32] Consequently within this article mechanisms which enable authorisation to be sought from the rightholder (namely through renewable payments) for each new access to or new use of a work in a legitimately-acquired form (for example, a software program on CD ROM), for authorization by the rightholder, namely through renewable payments. From that point on the user could not circumvent the technological protection linked to the work on pain of criminal sanctions, even if s/he has paid the appropriate payment with a view to gaining access. This extension of protection beyond traditional copyrights has already provoked comment in the United States.[33] In the final section we will examine this controversy, the issues and the terms of which are not so very different to the European situation indicated above.

*Types of illicit activities*

These new measures sanction both circumvention of the technological measure as well as the manufacture and marketing of devices which circumvent this protection.

In terms of circumvention the text will only be in force at the end of a period of two years from the date that these new measures take effect. Over these two years the *Register of Copyright* and the *Librarian of Congress* will examine how far this new ban on circumventing technical protection systems might cause prejudice to users of protected works, as well as to exceptions to copyright which generally fall under the **fair use** category, such as quotation, teaching, research, news summaries, etc. At the end of these two years some types of works might be exempted from the ban on circumvention of access systems which protect them, in order to allow a legitimate use of them. This would be the case, for example, for scientific articles, if it was considered that their frequent use in research means that users must be able to consult them, despite the technological protection which would be assigned to them.

The evaluation process on the effect of the ban will be repeated every two years.

The other branch of the protection of access systems is, for its part, effective immediately. It targets manufacture, imports, supply to the public, provision or any other type of marketing of technologies, products, services, devices or illicit components. Supply of services as well as products are both covered.

---

32 J. GINSBURG, *op. cit*., p. 159.

33 J. LITMAN, *New Copyright Paradigms*, http://www.msen.com/~litman/paradigm.htm; D. NIMMER, *Brains and other paraphernalia of the digital age*, Harvard Journal of Law and Technology, vol. 10, nº 1, 1996, pp. 1-46; J. GINSBURG, *op.cit.*

However, liability either of the person who commits an act of circumvention or a person who manufactures and distributes illicit devices is not dependent on their knowledge of the issues involved.

*Illicit devices*

Products or services will be considered to be illicit where they have been largely designed or manufactured with the aim of circumventing a technological measure, whether it is a question of controlling access or protection of an exclusive right, in those cases where there is only one reason for marketing this product or the use is limited to circumvention or where the publicity campaign has focused on the idea of circumvention.

*Exceptions to the ban on circumvention of access systems and on the manufacture of devices*

The American text was the subject of intense lobbying on the part of various industries and interested parties, from the computer and electronics industry to libraries. The ban on the principal of circumventing technological systems for controlling access has some exceptions which are often complex in their form. We will limit ourselves to indicating the main ones here:

- **exception in favor of non-profit-making libraries**: §1201 (d) provides an exception to the ban on circumvention to the benefit not only of libraries but also of archives and educational institutions which are not for profit. This exception is limited to the possibility of contravening a technological protection with the sole aim of gaining information regarding the potential value of buying the protected work. A copy of this work must not be otherwise available and the library must relinquish the copy of the work to which it gained access once its decision has been taken.

- **exception for authorities and security monitoring**: official authorities or police who circumvent technological protection during their investigations will not be considered to have committed a crime. This goes without saying, as does the exception in the context of checking the security of a system when this is carried out with the authorisation of the owner of the system or the computer network.

- **decompilation**: following the European directive on protection of computer programs, American law grants the legitimate user of a copy of a program the option of proceeding to decompilation of a program in order to ensure inter-operability. At present, systems controlling access could in effect destroy this possibility. Therefore the law allows an exception to sanctions for the circumvention of such technological measures in this context;

- **research activities in terms of encrypting**: §1201 (g) institutes a strict exception where circumvention is necessary in order to make progress in research in terms of encrypting, particularly in tracking and checking the weak links in the technology. Within this exception circumvention of access systems as well as development of illicit devices are exempt;

- **exceptions for minors**: the American legislative body is very concerned by the fact that minors may be able to have access to pornographic or violent content on the Internet. The industry has therefore developed several screening systems, such as PICS, [34]to respond to those concerns. During discussions held by the DMCA it transpired that these systems could contain components able to circumvent technological protection of access, specifically in order to check the nature of the content of the site visited. Section 1201 (h) stipulates that such systems cannot be banned from marketing simply for this reason;

- **protection of personal data**: insofar as access technology or the protected content also contains personal data relating to the user – **cookies**, for example – the former is given the tools to circumvent such technological measures in order to discover and to erase the component which contains these personal data unbeknown to the person concerned. The exception is, however, limited to this sole aim and cannot be applied if the operator of the technological system has informed the user of the data collection.

*Limitations on copyright and protection*

The DMCA does not rule on the status of acts of circumvention carried out to exercise an exception allowed within the context of fair use, but, as has already been noted, the legislator has set out a procedure for assessing the effect of the ban on copyright exceptions and limitations. Furthermore, the potential exemption of a protection for some exceptions will only extend to technological measures controlling access and not to measures which protect exclusive rights. However, since the circumvention of technological measures has not been banned within the context of protection of exclusive rights, this difference in the terms does not apply very often.

(ii) Protection of technological measures which safeguard copyright

*Protection aim*

Paragraph (b) of section 2101, the text of which was quoted above, aims more directly at transposing the WIPO treaties insofar as the technological measures considered here are in fact those which protect rights recognised through American copyright, whether it be rights to reproduction, adaptation, distribution, public performance or public display of the work. In this context the protection established is unique and targets manufacturers and suppliers of circumvention devices. The act of circumvention itself is not reprehensible but acts carried out later by the user will represent an infringement of copyright. It has obviously been considered that in this case there is no justification for a further sanction.

The technologies targeted are those which effectively prevent a right accorded to the holder of copyright by American Copyright. Reference is being made particularly here to SCMS and to other anti-copy devices.

---

[34] A. LIVORY, *CEE, contrôle du contenu circulant sur Internet : une approche particulière, le contrôle par l'usager et le système PICS, D.I.T.*, 06/1997, nº 97/2, pp. 52-54; Y. POULLET, Quelques considérations sur le droit du cyberespace, FUNDP, Faculté de droit, 1998, 27 pages.

Acts of illegal marketing are identical to those relating to the measures of controlling access, that is manufacture, import, supply to the public, provision or any other kind of marketing of technologies, products, services, devices or illegal components. The same goes for the definition of illicit devices, which is applied *mutatis mutandis* to both types of technology (of access and protection of rights). The essential criterion is also the marketing aim or a limited use other than that of circumvention.

*Exceptions to technological measures for the protection of rights*

Circumvention is not forbidden in itself where fair use is concerned. In this case the users may deactivate a technological protection to carry out such an act. On the other hand, nothing states that authorization is granted for producing and distributing circumvention devices with the sole aim of over-riding a protection system in order to use a work in the context of a granted exemption.

*Exceptions regarding the manufacture of illicit devices*

Only the exemption for those acting for the authorities or the police services can be applied equally in the framework of technological copyright protection measures.

*"No mandate" clause*

The DMCA stipulates that electronics, telecommunications and computing industries are not obliged to adapt their products so that they can interact with technological protection measures or access control systems. [35]

1.4. Australia: Copyright amendment (Digital Agenda) Bill of 1999

A bill is also being prepared in Australia with two objectives: to adapt Australian law on copyright to technological developments and to transpose WIPO's Treaties. As far as legal protection of technological measures is concerned the draft stipulates:

*(5B) A person must not provide a circumvention service if the person knows, or is reckless as to whether, the service will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.*

*(5C) A person must not:*

*(a) make a circumvention device; or*

*(b) sell, let for hire, or by way of trade offer or expose for sale or hire a circumvention device; or*

[35] Art. 1201 (c) (3).

*(c) distribute a circumvention device with the intention of trading, or engaging in any other activity that will affect prejudicially an owner of copyright; or*

*(d) by way of trade exhibit a circumvention device in public; or*

*(e) import a circumvention device into Australia with the intention of:*

*(i) selling, letting for hire, or by way of trade offering or exposing for sale or hire, the device; or*

*(ii) distributing the device for trading, or for engaging in any other activity that will affect prejudicially an owner of copyright; or*

*(iii) exhibiting the device in public by way of trade; or*

*(f) make a circumvention device available on-line to an extent that will affect prejudicially an owner of copyright;*

*if the person knows, or is reckless as to whether, the device will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.*

*Protection aim*

Effective technological measures which are the aim of this protection are defined as "*a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject-matter if, in the ordinary course of its operation access to the work or other subject matter protected by the measure is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright in the work or other subject-matter*".

Here once again the key element of the definition is access to the work and not the protection of a specific copyright. In contrast to American law, even European law, there is no protection planned in parallel for the technological protection systems which prevent reproduction or any other act of exploitation under copyright. The question of the possible application of this text to anti- copy systems or to other technologies where the main aim is not ensuring security and controlling access to the work must be raised once again.

*Prohibited acts and illicit devices*

Only acts preparatory to circumvention will be sanctioned and not the act of circumvention itself made by the user. Preparatory acts which are banned are offering circumvention services, the manufacture, sale, hire, public display with a view to sale, marketing, distribution, importing or making available on-line a circumvention device, this last being defined as "*a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than circumvention, or facilitating the circumvention of an effective technological measure*."

The criterion is similar to the European and American criteria.

However, for responsibility to be invoked it is laid out that a person who has infringed rights must have been aware of the circumvention use of the machine or device.

*Limitations on copyright and exceptions*

The Australian bill regulates for the first time the delicate question of the treatment of copyright exceptions. It is in fact laid down that the ban on manufacturing and distribution acts of circumvention devices or offering services will not be applied if the person who is provided with this service or device signs a declaration by which s/he commits to using it only with the aim permitted by law, this aim must be clearly mentioned on the declaration. The aim permitted by law is defined as a use of the device or service to carry out an act relating to an exemption under copyright or carried out on the authority of the rightholder. It appears that in this context a person could claim use of a circumvention device in order to carry out acts outside the area of copyright and through it could even free the provider of all liability in this regard. Therefore, it is to be feared that such a declaration might become common usage in supply contracts for such electronic devices which might in consequence render the manufacturers' liability almost nil.

Furthermore as far as manufacture and importing of such devices is concerned, no liability can be assigned to the manufacturer or the importer if their use is restricted to an aim permitted by the law.

*Exceptions to the ban on circumvention*

Apart from the general exception laid out in the case where it is a question of circumventing the technological measure to exercise an exception to copyright, the bill gives a general exemption to the ban for the authorities and the police services.

1.5. Other countries

To our knowledge Japan,[36] Singapore, Hungary and Ireland have either already transposed the WIPO Treaties in terms of protection of technological measures or are on the point of doing so. We do not, however, have the texts from these countries at the time of finishing this report.

Germany did also present a bill with the same aim which was designed to sanction circumvention, elimination and the destruction of technological measures, including computer programs, which protect copyrights.[37] This bill seems to have been abandoned by the new German government.

---

[36] Law of 15 June 1999.

[37] Proposal for the introduction of a fifth amendment to the German Law on Copyright of 7 July 1998, section 96a.

## 2. Protection of technological measures which monitor access to services

Legislation situated outside the narrow field of intellectual property does in some cases give protection to technological systems which could also be invoked by rightholders to protect their works, particularly to manage access to them.

The aim of these measures is usually to protect technological systems which prevent and control access to certain services. Such measures, which were in the past put in place for certain analog services in some countries,[38] could be taken up and broadened for digital and on-line services because of the merging of the audiovisual, information and telecommunications industries.

We will examine only one European directive which seems to us to establish extra protection for technological measures protecting access to protected works. This directive is 98/84/EC of the European Parliament and the Council on the legal protection of services based on, or consisting of, conditional access. The directive is dated 20 November 1998.

The objective of the directive is to protect services where access is dependent on certain conditions, particularly through payment of a fee, as well as to sanction the marketing of mechanisms which facilitate circumvention of conditional access systems. Protected services are namely radio and television as well as the services of the information society.

This could include video or audio services on -demand, electronic editing, access to an on-line database, a site containing music catalogues, etc. On the other hand, offline input mediums, where access would be regulated by a technological system would not be protected by this text.

Rightholders could therefore prevent the marketing of devices which enable the circumvention of access measures which they rely on. It is useful to note immediately that this directive does not aim to protect content which comes under intellectual property. The initial proposal moreover expressly excluded technological measures applied to works protected by copyright.[39] In its final version the directive states that its application will be made without prejudice to community measures concerning intellectual property as laid out in the directive on copyright in the information society (see above). This, however, does not answer all the questions on potential overlapping and on the interpretation of the two texts and the existence of a dual protection. In principle, the two directives have different aims: in the one case the work is being protected and in the other a service is protected, whether it is made up of protected works or not.

The directive on conditional access seeks to protect services with conditional access as well as technologies which guarantee and control this access. Insofar as the proposed directive on copyright defines technological measures such as those which monitor access to works, the two texts are likely to protect the same technologies, as well as to sanction the same types of pirate systems. We have to recognize that the vast majority of services of the information society will include works protected by copyright or related rights as well as

---

[38] As far as the encrypting of television programs is concerned, we quote articles 79-1 to 79-6 of the French Law of 30 September 1986 relating to freedom of communication, articles 297 to 299 of the English Law on Copyright, article 605 of the United States' Communications Act.

[39] Preamble 15 of the proposal for a directive, 98/84/EC

protected databases. A database where access is ensured through a technological measure will constitute both a work (or a protected object) and a service with conditional access. The protection will therefore be dual. [40]

The criterion of paying for a service also appears to be essential for the implementation of the directive on conditional access. However, this does not mean that payment should be made before the service is provided, nor that it should be at a fixed rate. Thus a service with conditional access consisting of an on-line collection of photographs associated to a **metering mechanism** could be protected, even if the invoice which includes payment according to the exact number of uses of the photo library is sent at regular intervals after initial access.

The directive on conditional access imposes a duty on Member States to forbid manufacture, importing, sale, distribution, hire, possession for a commercial aim, installation, maintenance or the replacement of a device which allows unauthorized access to a protected service, or the promotion of such devices or machines. The criterion of unlawfulness of devices for unauthorized access to protected services is stricter than for technological measures in terms of copyright. Only equipment or software designed or adapted in order to allow such access will be prohibited.

Certainly the fact that protection of services with conditional access lies outside copyright and related rights prevents exceptions and limitations under copyright being invoked in order to dismantle technological protection. Thus a service with conditional access including works in the public domain could be protected by a cryptographic mechanism. Those who use this service could ban the manufacture of pirate decrypting keys, probably not on the basis of the future directive on copyright but certainly on the basis of transpositions of the directive on conditional access. The fact that targeted works do not have protection under copyright would not, in the end, matter greatly.

Consequently, rightholders sometimes would be well advised to invoke this text in order to prevent the sale of circumvention systems: exceptions and limitations on copyright could not be raised as a counter argument. Furthermore, within the context of the directive on conditionalaccess some activities such as maintenance, installation or replacement of such a measure are explicitly sanctioned, which the draft directive on copyright does not allow for.

## 3. Measures relating to computer crime

Unauthorized access to works or other protected objects can, in some cases, be included in an offence, which causes prejudice to computerized systems. Such infringements can be found in many countries' Criminal Codes under the section on elimination of computer crime, particularly following concerns which reached the light of day in the 1980s when hackers and other computer technology pirates first appeared.

The Council of Europe recommended criminal punishment through specific measures of a series of acts which negatively affect systems and computer data.

This list specifically included the following acts:

---

[40] S. DUSOLLIER, *Electrifying the fence…, op. cit.*, p. 290

- Computer fraud, defined as "*the entry, alteration, deletion or elimination of data or computer programs, or any other interference in computer processing, which influences the result by causing economic or material prejudice to another person with the intention of obtaining an illegitimate economic advantage for oneself or for anyone else or with the intention of illegally depriving this person of his/her property*".

- Forgery in computing which consists of the traditional offence of forgery through interference in a computer system;

- Material damage affecting data or programs which consists of deletion, damaging, deterioration or elimination of data or of computer programs without authorization, the most widespread case of this being, of course, viruses or other computer bombs;

- Computer sabotage which is entry or interference in computer systems with the intention of preventing its operation

- Unauthorized access to computer systems made by violating security regulations

- Unauthorized interception of computer communications

- Unauthorized reproduction of computer programs or topographies

- Alteration without the right to of data or computer programs

- Computer espionage

- Unauthorized use of a computer, a system or of a computer network. This is a crime only in some cases;

- Use without right of a computer program.

Although some of these offences are completely alien to the hypothesis of technological protection of works, others could, in a subsidiary fashion, serve as a basis for a case against actions taken to circumvent the technological barrier.

For example, someone who contravenes the cryptography system which ensures secure access to a data base of protected works could be prosecuted for computer fraud (the prejudice caused to rightholders through entry into the system resulting in loss of fees owed to them, although fraudulent intent would need to be proved), as well as on the basis of an offence resulting from unauthorized access to the database.

Circumvention of a watermarking mechanism which was to prevent the modification of the work could also be sanctioned as a crime of unauthorized alteration of data. Circumvention of a technological measure ensuring safe access and use of a computer program would be grounds for the offence of unauthorized use of a computer program. However, this particular infringement has generally been included by national legislators within the context of legal protection of computer programs and not in penal texts specifically relating to computer crime.

Countries which have followed the recommendations of the Council of Europe have for the most part introduced into their penal arsenal an offence of unauthorized intrusion and of data alteration. As far as unauthorized access is concerned, let us quote article 321-1 paragraph 1 of the French penal code which punishes fraudulent access and maintenance of a computing system, and article 202a of the German penal code which bans obtaining data which has been specially secured from unauthorized access. Norway [41] and Finland also sanction a violation of security regulations. In contrast, American federal law[42] in this area, requires that, beyond illegal access, obtaining, modification or destruction of information must have taken place.

The matter of fraudulently maintaining the system which can be found in French legislation would also specifically allow for cover for the circumvention of technological measures relating to the use of protected works, even where access itself has been authorized by the rightholder. Let us take as an example a person who has a membership for a video service on-demand where billing is made for each time the service is used at a later date. The person manages to circumvent the technological measures which record and bill for this use. In our opinion, circumvention of the technological system would represent an inappropriate maintenance of the data processing system which would be punishable under French law.

As far as alteration of data is concerned, namely removal of the digital marking on the work would be a crime under article 303a of the German Criminal Code as well as under article 323-3 of the French Criminal Code.

## C. FINAL CONSIDERATIONS

Since adoption of the WIPO Treaties three years ago, some countries have transposed regulations on legal protection of technological measures into their national law or are at least preparing to do so. This clearly demonstrates how vital such new protection has become.

Furthermore we have been able to recognize that despite some divergences in the scope and the conditions of protection, national or regional measures agree on the fundamental elements of an adequate system of protection, such as the definition of the object to be protected, the delimitation of illegal acts (both the act of circumvention and the making available of circumvention mechanisms) as well as the definition of illegality of these mechanisms (items 1.1, 1.2 and 1.3 hereinafter, respectively).

Some questions remain unresolved, however, the most delicate certainly being the existence of potential conflict between legal protection of the technological measure and exceptions and limitations of copyright (item 2 hereinafter).

---

41 Article 145 of the Norwegian Criminal Code

42 Federal counterfeit access device and computer fraud and abuse. Act of 1984, USC title 18, chapter 47, § 1030.

## 1. Components for an effective and adequate system of protection

### 1.1. With regard to the protection aim

The definition of technological measures where circumvention should be forbidden was left to the discretion of States transposing the WIPO Treaties. The only indication was that these measures should have the aim and function of protecting rights belonging to the author or to another rightholder. Therefore at first sight it was a question mainly of protecting technologies which prevented reproduction or communication to the public of works or of protected contributions. However, States and regional organizations, such as the European Union, have generally introduced or adopted texts where the object was not only technologies which protected copyright in a strict sense, but also technologies which control access to works or on which access is dependent. This is clear in the American and Australian texts, it also apparent in the definition of technological measures set out in the community proposal.

Therefore technological protection of access to a work becomes safeguarded insofar as its circumvention is forbidden, which provides a *de facto* protection of access to the work, where monitoring would therefore become a prerogative of the rightholder without this being necessarily stipulated by law. It is true that a large majority of technological systems being used to protect works are measures based on cryptography which, in the first instance, prevent unauthorized access to the encrypted content. Access to a work alone, which would have required dismantling a technical barrier, without an act allowed under copyright taking place after the access, would fall under the gavel of sanctions.

This extension indicates clearly how essential access to a work is for rightholders. Jane Ginsburg has noted that: "*access probably will become the most important right regarding digitally expressed works, and its recognition, whether by the detour of prohibitions on circumvention of access controls, or by express addition to the list of exclusive rights under copyright, may be inevitable*.".[43] It has, however, led to some confusion in transpositions of the WIPO Treaties in this regard and in some cases has led to a hybrid protection where the line between protection of rights and protection of access to works is unclear. The protection of systems monitoring access seems, in fact, to go beyond the scope of the measures in the WIPO Treaties.

The concern to protect technologies relating to access can be perfectly understood. However, it falls more under protection of access to the service containing the works and particularly lies within protection of remuneration of a service. It is therefore a concern more for the exploiter or the distributor of the works than a question of direct protection for rightholders. The interest protected through legal protection of technological measures is linked to the distribution of works on the networks. This interest certainly deserves to be protected, as does, for example, that afforded by the European directive on conditional access. But it must be recognised that this protection cannot be exclusively justified on the grounds of considerations related to intellectual property. This displacement of the real reason behind having technological and legal protection should, at the very least, be the subject of more serious reflection.

---

[43] J. GINSBURG, *op. cit.*, p. 171.

1.2. With regard to types of activities which are illegal.

Where the WIPO Treaties only target in the first instance the very act of circumvention itself of technological protection measures, national measures which we have looked at have unanimously banned circumvention by a general prohibition on the manufacturing and the distribution of devices enabling or facilitating such a circumvention. It seems, of course, clear that large-scale distribution of mechanisms which can undo technological protection systems will cause a greater prejudice to rightholders than isolated acts of circumvention. In some cases protection put in place in this way by countries is limited, moreover, to so-called preparatory acts, to the exclusion of the circumvention activities themselves. This is particularly the case in Australia and the United States and as far as technological measures protecting copyright are concerned.

Furthermore, it is regrettable that most texts are not clearer on activities concerning the distribution of circumvention devices. Thus, supply on a web site is not explicitly singled out, just as the unlocking systems made freely available and without thought of monetary gain are not targeted. In most cases where pirates have "cracked" technological protection they have, in fact, given details of how they have done so a few hours later through the Internet without seeking financial gain. However, the protection set up in the United States and in Europe seems to be great enough to include distribution acts other than those carried out within a marketing context.

1.3. Description of illicit devices

The question of knowing at which point a device which allows the circumvention of technological measures becomes illegal is difficult to determine. Certainly the interests of the electronics and computing industry must be taken into account. They would not wish to see some of the devices that are developed banned simply because some users employ them to undo the technological protection. It is difficult to strike a balance. We have seen that most of the measures which exist refer to the criterion of the marketing purpose or to limited use. Forbidden devices will be those which have no other marketing aim or only very limited use beyond circumventing the protection, which leaves reasonable room for manoeuvre for the judges who must put these measures into effect. The promotion and marketing of measures with an explicit aim to circumvent are, of course, also targeted. In conclusion, the line between legal and illegal devices as given here, is logically based on the evidence of the aim of the device which has been designed, produced, promoted or sold.

Of course the parameters of this criterion are still liable to many interpretations which the legal system must clarify. It is nonetheless important to highlight the value of defining the illegality of circumvention devices in identical manner in many countries.

## 2. Limitations of copyright and exceptions

The question of the conjunction of exceptions and limitations to copyright and of legal protection of technological measures represents one of the most complex points of the issue. It is clear that a technical measure can, by definition, by locking access to a work or by preventing the carrying out of an act which requires the author's authorization, greatly restrict the ability of the user to carry out acts which are permitted through a legal exemption. If, after using a technical protection the user is no longer enabled to quote from a work, to make

a private copy of it, to use it for educational reasons or for information, then the extent of these exceptions in the digital world is likely to be seriously reduced.

In the context of protection of technological measures the question has two aspects to it. Since States have generally instituted a dual protection for technological measures, both with regard to its circumvention and the availability of illegal mechanisms, the incidence of exceptions must be envisaged in terms of both branches of this protection.

Firstly, the question that could be asked is whether the act of circumvention of the technological measure is forbidden in the same way if it is carried out in order to have access to an unprotected work or to carry out acts covered by an exemption.

Secondly, some manufacturers or distributors of systems allowing the circumvention of technological measures are sometimes tempted to cite the fact that their devices have only a perfectly legitimate aim, namely to allow users to go past the technical barrier in order to have access to works in the public domain. We will begin by analyzing this second aspect of the question before looking at the trickier one which relates to the situation of exceptions, given the ban on the act of circumvention.

### 2.1. Exceptions and the manufacture of circumvention devices

As far as the ban on so-called preparatory acts prior to an act of circumvention is concerned, the issue of exemptions is summarized into the question of the potential tolerance of systems which only allow circumvention in order to access unprotected content or in order to exercise a right to an exemption recognized by law.

Where technological measures of protection relate indiscriminately to protected works and those which are free of rights, the measures supposed to circumvent them will also do so in an indistinguishable fashion. It is difficult to imagine that a device might be designed only with the aim of carrying out private copies or copies of an unprotected work. It is clear that the same systems will allow circumvention of protection mechanisms for illicit aims. Furthermore, authorizing only systems used for legitimate aims to be circulated would allow their manufacturers to consistently abdicate all responsibility.

The answer seems to be relatively simple to us. The designers and distributors of devices which allow the circumvention of protected works, even if their use is likely to be limited only to the unlocking of the access to non-protected works, would not be able to escape the ban on this basis alone. Nothing, however, prevents designers to negotiate with their rightholders the authorization of systems relating to specific unlocking mechanisms, for example for security control systems. In the case of libraries which so desire, provided the law permits, a back-up copy could be made or archived.

### 2.2. Exceptions and the act of circumvention

The user who wishes to exercise his right to an exemption will sometimes be forced to unlock the technological protection which prevents it. If we believe that this type of circumvention is illegitimate, the user will be punished even if he is outside copyright and cannot be prosecuted on that basis. This would seem to demonstrate that the object of the

protection is more the technology itself than copyright, because of the investment in manufacturing and in its use. If, on the contrary, this circumvention is considered to be legitimate then the user will not be prosecuted either for violation of copyright or for violation of the protection of the technological measure, which then raises the question of determining the aim which was intended by the user during the circumvention. In actual fact, how can one demonstrate that circumvention of the protective technology has been carried out only to exercise a right to an exemption?

The solution which is often proposed in this situation is to give exemptions an inflexible nature, which cannot be circumnavigated either by contracts or by technological measures. [44]

This solution is, however, only partial. The technology is, in fact, blind and only responds to requests for technical acts such as a copying, printing, despatching, reading or access. It cannot recognize the context in which such an act is carried out. The conditions which are often subjective placed on the exercise of an exception cannot be analyzed and recognized by such technological measures. An example is the inflexible nature given within the European directive on exempted databases which allow the legitimate user to carry out acts necessary for normal use. How can the technological measure which protects the database determine what is normal use?

In the same way an equally strict exemption, is granted to the user of a database protected by a *sui generis* right to extract non-substantive sections. The system protecting the base would not be able to define what is a non-substantive section unless it has been programmed to that effect by the rightholder, which would remove a part of its exceptional nature.

Another solution can be found within the framework of contractual relations between rightholders and users. The authors can either provide certain types of users who have legitimately acquired the work with a copy of it without the technological protection or could provide a copy where the technological protection takes into account the type of particular exemptions for which users qualify. This solution would only concern, however, large categories of users, such as libraries, journalists, researchers, teachers, who are accorded particular exceptional rights. These same users could benefit from a type of presumption which exempts them from the ban, a presumption which should be reversed by rightholders in the case where such users have circumvented the technical protection outside the context of the limitations on copyright which usually apply. However, individual users who were not granted this option would be penalized by these different possibilities. The system of exemptions would no longer be anything other than a matter of contractual negotiation between the eligible parties and some users we could describe as collectives.

These solutions can only be used as a basis for consideration of the particularly delicate issue of exceptions.

[End of document]

---

[44] B. HUGENHOLTZ, *Rights, Limitations and Exceptions: Striking a Proper Balance*, Keynote Speech at the Imprimatur Consensus Forum, 30/31 October 1997, Amsterdam; L. GUIBAULT, *Contracts and Copyright Exemptions*, Amsterdam, Institute for Information Law, 1997.