

An introduction to the state of the art of the technology of protection of copyright and its legal protection

1. Introduction

During the 'industrial era', goods and services destined for educational, cultural, information and leisure purposes were supported by means like print, television, and audiovisuals in general. These goods are very suitable as primary material for e-commerce. The price of the physical support products for these goods and services largely consists of production and distribution costs, only a small proportion of the price is revenue destined for the authors and intellectual proprietors, and business people organising the production of these goods and services.

Nowadays, the majority of business to consumer (B2C) transactions concerns immaterial products that can travel over the Internet, directly to the personal computer of the consumer. This type of online distribution currently is being used in various branches in the realm of Intellectual Property, for example:

- Online press publications on Internet pages linked through hyperlinks, accessible with search engines, thus offering dynamic reading facilities.
- A large number of radio and television stations which broadcast their programs in whole or in part on the Internet.
- Online distribution of music in digital formats.
- Online distribution of cinema and TV, which, in mid term, will encompass interactive TV in the light of the PC and TV convergence.
- Software programs, downloadable from the Internet.

The digital presence and distribution of these documents and sources has significantly increased infringements of copyrights protection intensified related problems. The problems arise from the intrinsic value of digital data i.e. easy, cheap and quick to copy, with moreover a copy indistinguishable from the original. The protection of intellectual property rights thus is to be viewed as a prerequisite for the successful implementation of electronic commerce solutions seeking to distribute digital content.

This paper shall cover two main topics with regard to the technological measures. Firstly, the different protection technologies shall be examined. In the second part, some thought shall be given on the legislation at international and European level with regards to the referred technological measures.

2. General considerations for Copyright Protection On-Line

2.1. Technological measures.

The so-called "technological measures" are "insert", like, for example:

- Measures that make impossible to copy archives from a memory space in a Computer.

- Measures that make impossible to print digital texts.
- Measures that permit identification of work protected by copyrights and show their terms and conditions of use.

2.2. Electronic information about the management of intellectual property rights.

It is understood for "Electronic information about the management of intellectual property rights", regarding the sectors that encode digital archives, which, during their processing by a PC, allow to:

- Manage databases with information concerning the protected works.
- Register transactions related to these works, in order to e.g. simplify legal proof issues.
- Facilitate adequate electronic payments features i.e. micro payments.

3. Helicopter view of technology

Technological mechanisms will progressively allow access and transmission of works to be secured and to supplement the legal protection with efficient technological protection. The goal to be achieved is to deter the threats of technology by using technology itself. As one author has aptly put it, "the answer to the machine is in the machine".¹

The technologies likely to be used by authors and other right-holders to protect their works and performances in the information society are quite different. Some have been specifically designed to answer the digital threat to copyright, while others have been developed to protect indiscriminately any kind of digital content, whether copyrighted or not.

It is beyond the scope of this article to draw up a specific list of technological devices either in current use or in course of development, just as it is impossible to predict the future of such technologies in the area of protecting works under copyright.²

It is possible, however, to sort technological devices for copyright and neighbouring rights protection into four broad functional categories of these devices. Thus, we may distinguish between measures that efficiently protect an act falling under the author's exclusive right, systems of access control, tools for marking and identification and electronic rights management systems.

3.1 Technological protection of copyright

These are technical tools which prohibit the performance of any act or use that is the exclusive right of the copyright holders, such as printing, transmission to the public,

¹ Clark, C., *The answer to the machine is in the machine*, The Future of Copyright in a Digital Environment, pp. 139-146. See also Burns, C., *Copyright Management and the NII: Report to the Enabling Technologies Committee of the Association of American Publishers*, May 31, 1995.

² Gervais, D., *Electronic Rights Management and Digital Identities Systems*, WIPO Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, First Session, Geneva, 14 and 15 December 1998.

digital copies, modifying the work, etc. Anti-copying systems are above all those whose main function is to prevent the making of a copy of a protected work or object, either solely digital or any copy whether digital or analogue.

For example, Dongles are a means of protecting software with a hardware device for ensuring that only authorized users can copy or use specific software applications. All software protected by this system then connects to this key to verify what the user's rights include. The dongle seems like a precursor of smart cards, which allow a greater amount of information to be stored. Smart cards may also contain prepaid payment units. Unlike dongles, whose use until now has been limited to expensive software programs, smart cards will no doubt be used more often for software as well as for other works available to the general public.

The Serial Copy Management System is a system used mainly in the United States on audio-digital recording devices such as DAT and mini-discs. The DAT-player allows making a digital copy from the original but will not allow a further copy of such copy if the original's copy protection is enabled. The technique therefore prevents unauthorized copying to the extent that a DAT-copy cannot be further digitally copied with a DAT-recorder.³

3.2 Access Control

One of the major challenges of digital networks is to make access to protected information and content secure, both in order to ensure payment of a fee and to protect the copyright covering the work that has been thus "padlocked".⁴

Many systems have accordingly been developed with a view to ensure and secure access either to a work or a collection of works, or to a service including among other things the works under copyright. Deactivating the access control device is done either by payment or when other terms of permission agreed with the copyright holders have been met. The access device may control only initial access and subsequently leave the work free for any use, or it may check on the occasion of each new access to make sure that the terms have been respected.

There are different technologies to do that: cryptography, passwords, set-top boxes, black boxes, digital signatures and digital envelope. The cryptography process is well known. Encryption works by encoding the text of a message with a key. In traditional encryption systems, the same key was used for both encoding and decoding. In the new public key or asymmetric encryption systems, keys come in pairs: one key is used for encoding and another for decoding. In this system everyone owns a unique pair of keys. One of the keys, called the public key, is widely distributed and used for encoding messages. The other key, called the private key, is a closely held secret used to decrypt incoming message. Under this system, a person who needs to send a message

³ Kaestner, J., *Law and Technology Convergence: Intellectual Property Rights*, ESPRIT Project 27028, Electronic Commerce Legal Issues Platform, 16 December 1999.

⁴ Dusollier, S., Pouillet, Y., Buydens, M., *Copyright and Access to information in the digital environment*, a study prepared for the Third UNESCO Congress on Ethical, Legal and Societal Challenges of Cyberspace Infoethics 2000, Paris, 17 July 2000, pag. 21.

to a second person can encrypt the message with that person's public key. The owner of the secret private key, making it safe from interception, can only decrypt the message. This system can also be used to create unforgeable digital signatures.⁵

Most practical implementations of secure Internet encryption actually combine the traditional symmetric and the new asymmetric schemes. Public key encryption is used to negotiate a secret symmetric key that is then used to encrypt the actual data.⁶

Digital signatures are a particular application of public key cryptography. In the context of copyright protection, unauthorised persons mainly use this technology to secure transmissions of works over electronic networks and to prevent access to the work. The decoding key is provided after payment of the fee or fulfilment of other conditions for using the work.⁷

The digital envelope or digital container is an application of cryptography through which a work is "inserted" into a digital envelope containing information regarding the work and its terms of use. Only after having satisfied these terms (such as payment of a fee, use of a password, and so on) does the envelope actually open and the user gains access to the work.

3.3 Tools for marking

Some techniques can be used to identify and mark works. The techniques have various purposes: the main one is to serve as a visible or invisible means of inserting information about the work, whether it could be the title of the work, the identity of its creator and the copyright holder, or the terms of use.

Here, the concern is mainly with watermarking or tattooing, which allows certain information to be discreetly inserted into the work's digital code. This marking is usually invisible and inaudible. Using a Steganography technique makes the invisible inscription. Originally, the "art" of stenography has been used to communicate with another through seemingly harmless messages, which contain hidden secret data.⁸

In a digital environment, watermarking alters certain "unnecessary" bits of an image or a sound. Using an appropriate software program, this digital code may be extracted and deciphered. The marking is normally indelible and is to be found in every part of the work.

⁵ Stein, L., Stewart, J., *How does encryption work*, <http://www.w3.org/Security/Faq/wwwsf5.html#CON-Q9>

⁶ More information on public key cryptography can be found in the book "Applied Cryptography", by Bruce Schneier.

⁷ Dusollier, Pouillet, Y., Buydens, M., *Copyright and Access to Information*, 2000, p. 22 *Op. cit*

⁸ Johnson, N., F., *Steganography*, <http://www.jitc.com/stegdoc/sec201.html>

However, other characteristics of these technologies provide copyright protection somewhat indirectly. By marking is in certain cases perfectly visible; a “mark” is then clearly placed on the representation of the work.

Further, each separate copy of the work distributed to users may also incorporate a distinct digital serial number. In that case, a pirated copy later found on the market can reveal the original copy from which the counterfeit was made. By thus stamping each image, it is possible to trace unauthorised copies of the image back to the source by using a file repeating the serial numbers and the users to whom these stamped images have been licensed. Here the essential function of the protection technique is to provide proof of counterfeiting. Finally, one last useful function of watermarking is for the purpose of authenticating the marked content, notably as a guarantee that the work is present in its entirety.

3.4 Electronic management systems

Electronic management tools are all technologies that ensure rights management over electronic networks by making possible to license online utilisation of works, and to monitor such use. These devices blend contractual and technological protection.⁹

Other functions may also be included in these tools: distributing royalties, payment related functions, profiling users, and so on. For instance, electronic agents have recently appeared on the market.¹⁰ Developed to perform many tasks on electronic networks, some of them are even programmed to negotiate and sign electronic contracts.

Another possibility is the distribution of royalties to authors and performers and other copyright-holders online via such agents. When these agents merely control the utilisation of works and keep tabs on how frequently works or websites are consulted, or even draw up precise profiles of the users, the term often used is metering systems.¹¹

Finally, Electronic Rights Management Systems (so called ERMS) consist rather of a combination of many tools and technologies designed to play several roles.¹² The term may cover all systems where the provision of content is connected to certain requirements such as registering, technological measures, standard licensing terms (“click-wrap” licensing conditions) or similar.¹³

4. An approach to the Legal protection.

⁹ Hugenholtz, P.B., *Copyright, contract and technology – What will remain of the public domain?*, in *Le Droit d’auteur: un contrôle de l’accès aux oeuvres?*, Cahier du CRID N. 18, Bruylant, 2000.

¹⁰ See Gonzalo, S., *A business outlook on electronic agents*, 2000/7

¹¹ Dusollier, S., Pouillet, Y., Buydens, M., *Copyright and Access to Information*, op. Cit.

¹² Vinje, T., *A brave new world of technical protection systems: will there still be room for copyright?*, E.I.P.R., 1996/8, p. 431.

¹³ Kaestner, J., *Law and Technology Convergence: Intellectual Property Rights*, op. Cit., p. 55.

The WIPO, in the WIPO treaty on copyright and the WIPO treaty on performances and phonograms gives legal remedies against modification or removal of these digital identification media.

For example, article 11, obligations concerning technological measures, of the WIPO copyright treaty states: Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Bern Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law.

The basic principles for technical resources regarding the legal protection of the information for the administration of the intellectual property are laid down in article 12 (Obligations concerning Rights Management Information) of the WIPO treaty on copyright and article 19 of the WIPO treaty on performances and phonograms.

The incorporation of these treaties has already led to significant changes in some legal orders. The USA, for example, in Title I of its 'Digital Millennium Copyright Act' of October 1998, have included norms for the protection of technological measures and for the information for the rights management, in line with the principles laid down in the WIPO treaties of December 1996.

On European Community level, article 6 of Directive EC/29/2001 of the European Parliament and the Council, 22 of May 2001, hereafter 'the Directive', harmonises aspects of copyright and of copyrights related to the Information Society. The Directive recommends the implementation by the member States of an adequate legal protection against the elusion of whatever technological measures effective, understood as: "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the right holder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholder's through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective".

In this way the European Community regulations establish a mandatory legal requirement for the member States to assure adequate legal protection against "any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright

or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.”

In the Spanish legislation, the incorporation of norms regarding the technical measures, in relation to digital technology, is well known in computer programs. For instance, Article 102. c) of the Law on Intellectual Property and Article 270, 3rd paragraph of the Spanish Penal Code.

From the above we can draw the conclusion that the regulation of this matter is principally done through prohibitive clauses. Regarding the principle of legality and prohibition, analogue to the field of Penal Law, the legislators should guard detail with typifying and categorising infracting behaviour, as well as with the exceptions. This should be done in such a way as to cover all measures protecting a legally protected intangible value.

5. Conclusions

The statement that the legal developments are leaping behind the reality in the digital world really is not very daring. The peculiarity of the discussed above is that the legislator should seek to protect not only an adequate protection of publications on the Internet, but also regulate the technological measures protecting these publications. Without prejudice to adapting the law to the needs of the information society, the rights of the author should evolve progressively with the development of a legal regime which remains secure and beneficial to both authors and consumers, through the creation of legal databases and the use of more efficient and compatible technological resources.