ALAI 2001 Congress, New York, June 13-17:

Adjuncts and Alternatives to Copyright

Session I.C.

Situating legal protections for copyright-related technological measures in the broader legal landscape: ANTI CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT

General Report

Séverine Dusollier*

INTRODUCTION

Following the development of the digital era and of security technology, anti-circumvention provisions have been recently integrated in the copyright scenario. But such provisions and technological measures of protection are not unprecedented. They recall other legal attempts to regulate the technology and the erection of technical fences around information and communications. Outside copyright, policies already prohibit the defeating of technical security systems. The purpose of this report is to assess the diverse legal techniques that complement anti-circumvention provisions related to copyright and that could help prohibit the bypassing of a technical fence.

Our mission has led us[1] into *terra incognita*, onto less frequented paths by copyright lawyers: broadcasting law, telecommunications, computer crime, liability and tort law, trade secret protection were the continents where we have traveled. Other less relevant legal provisions could be the atolls of a fifth anti-circumvention continent. We shall omit such protections[2].

---

* Séverine Dusollier is Maître de Conférences at the University of Namur (Belgium) and project reseacher at the CRID (Center of Research in Computer and Law).

[1] This report has benefited from the national reports. I thank therefore the national reporters : P. Wand (Germany), D. Lindsay (Australia), A. Cruquenaire & P.Y. Potelle (Belgium), N. Landry (Canada), P. Schønning (Denmark), N. Smith (United-States), R. Avilés Carceller (Spain), K. Sorvari et T. Ryhänen (Finland), G. Vercken (France), P.A. Koriatopoulou (Greece), A. Pojaghi (Italy), Kentaro Endo and Hiroshi Saito (Japan), G. Larrea Richerand, M. Larrea Legorreta, R. Larrea Soltero, C. Peralta Casares, O. Lecona Morales & F. Campuzano Lamadrid (Mexico), N. Helberger, B. Hugenholtz, K. Koelman, J. Seignette, R. Stuyt & D. Visser (the Netherlands), Paul Brügger (Switzerland), H. Best et R. Treagar (the United Kingdom).

[2] The national reports mention provisions in privacy and data protection or the principle of unjust enrichment. One could also think of the protection of the digital signature. All these provisions should be further considered.

Our journeys were guided by two viewpoints. In each of the territories we crossed, we had to gather the legal provisions that could be of some help to authors when either a protecting technical mean has been circumvented, or circumventing devices are offered to the public. This viewpoint runs along copyright-related circumvention provisions that traditionally prohibit both the *act* of circumvention and the *devices* that could help or facilitate the circumvention[3]. We will see that the distinction between act/devices is not so straightforward in extra-copyright regimes, but that it still makes sense since it concerns two different motives and two different forms of behavior.

In the first section of this report, relevant provisions outside copyright law will be addressed. Copyright will be ignored, but we shall returin to it in the second section where we will consider the likely relationship between copyright and extra-copyright anti-circumvention provisions in the light of the WIPO Treaties of 1996.

1. OVERVIEW OF ANTI-CIRCUMVENTION PROVISIONS OUTSIDE COPYRIGHT REGIME

1.1. Private Law : Liability, tort law, unfair competition practices.

a. Introduction

Civil law provides a manifold remedy against circumvention of technological measures, either under the contract law, or by liability and tort law. Such protection offers a particularly fragmented approach, especially since legal traditions and principles in that field vary greatly from country to country. An in-depth comparison of differences between tort legal systems would go far beyond the scope of this report.

However, national reports emphasize a consistent feature: the circumvention of a technological measure or trafficking in circumventing devices could be a fault, a negligence, a tort or an unlawful act, according to the relevant liability regime, thereby justifying compensation of the harm. As an illustration, the publication of a method to tamper with a descrambler so as not to pay the normal fee is an unlawful act according the Dutch *Hoge Raad*[4].

National reports underline some difficulties. The Belgian report says that the evidence and the evaluation of the damage will sometimes be difficult to make, particularly where distribution of the works, following the circumvention, has not taken place. The Australian report underlines that there is no clear principle for determining liability for negligence in cases of *"pure economic loss"*.

---

[3] Actually, what is prohibited is the manufacture or sale of the devices and not the devices themselves. But, in this report, for reasons of clarity, we will use the distinction act/devices.

[4] See the Dutch report.

Establishing the causation between the fault or tort and the damage is not without difficulties either, especially concerning circumventing devices[5]. The link between the sale of circumvention devices and copyright infringement could be in some cases difficult to establish.

In countries other than France or Belgium where any forms of socially unacceptable behavior may legitimate a claim for compensation, circumvention or preparatory activities must be covered by one of the various heads of tortious liability, such as negligence or trespass. As a condition for liability in negligence in common law and some other regimes, the plaintiff must show that the "circumventer" or the provider of circumventing devices owed him a duty of care. In circumvention cases, this requirement might not be met. The US report mentions a case where the sale of circumventing devices is a tort, if the seller had specific knowledge of their intended use.

Trespass, that can be defined as a wrongful interference with a person or with his possession of land or goods, is another head of common law liability. However, trespass can not easily be transposed to the digital world[6]. The main reason is that information is not normally deemed a good[7]. However, trespass on a publicly available website has been successfully claimed in a recent US case[8]. This could represent the beginning of better days in the digital environment for this legal technique. By the same token, it might provide protection against any act of unlawful circumvention of a technical fence.

There is not much case law where remedy for circumvention activities has been claimed under tort law. The diversity of the liability regimes makes it difficult to assess the overall ability of this technique to solve the problem of circumvention. It might be easier to turn to special concepts of liability such as the *unfair competition* or to the notion of *contributory infringement*, where case law is more prevalent.

b. Unfair competition practices

German case law abounds in court decisions where the trafficking in circumventing devices has been considered as an unfair trade practice[9]. The German Unfair Competition Prevention Act has been particularly applied to devices enabling the circumvention of technical protection applied to software. Offering programs for circumvention has been held as harmful to the business of a competitor, fair

---

[5] See the French and Belgian reports.

[6] D. L. BURK, "The Trouble with Trespass", *Journal of Small and Emerging Business Law*, Vol.4, Spring 2000, n° 1, p.27-56.

[7] See the Australian report.

[8] *eBay, Inc. v. Bidder's Edge*, (N.D. Cal. 2000), no. c-99-21200 RMW ENE

[9] German Report. See also: LEHMANN M., "Copyright and technical protections- German report", in *Copyright in cyberespace*, ALAI Study Days, June 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p. 371-372; A. RAUBENHEIMER, "Increasing importance of hardware locks (dongles) in recent German case law", *Information & Communications Technology Law*, Vol.7, No. 1, 1998, p.51-70

competition or the organization and operation of an enterprise. Distributing devices that circumvent anti-copy systems or hardware keys emulating the original key (*dongle*) have been condemned. The very act of circumvention has also been deemed as unfair competition when the computer programs devoid of the technical protection, have been eventually offered to the public[10].

Other countries have applied this technique for prohibiting illicit descramblers for encrypted television programs[11]. The same principle could be applied to circumvention devices.

It should be noted, however, that unfair competition law normally requires a competitive or parasitic relationship. It implies that offering circumvention methods or tools on the Internet free of charge and not in the course of a business could not constitute unfair competition.

c. Secondary liability

The United States knows secondary liability either as *vicarious liability* or as *contributory liability*. Case law has sometimes considered the activities preparatory to circumvention as a copyright contributory infringement. Video-game platforms are often dedicated to proprietary games. The platform can only play the games it acknowledges as its own brand. In *Sega v. Maphia*, manufacturing and commercialization of means to disable this technical process of acknowledgement have been deemed a *contributory infringement*[12].

However, the Supreme Court, in the Betamax case[13], limits such a liability for indirect infringement when the devices that could help infringe copyright are capable of other substantial non-infringing uses. The Betamax case opposed the movie industry to Sony and other consumer electronics manufacturers. The litigation evolved around whether video recorders were infringing copyright since they enabled reproduction of audiovisual works. The underlying issue was the balance to be found between the protection of a monopoly and the freedom of other businesses. The question, i.e. to what extent parallel and, at first sight, lawful commercial activities may lead to compensation for damages, is rather similar to unfair competition in Europe. The Supreme Court has ruled that Sony could not be held contributorily liable for its devices, even though they are a means to facilitate copyright infringement, if they are "*capable of substantial non-infringing uses"*. This standard of liability, also called the doctrine of the *"staple items of commerce"*, therefore restricts cases where trafficking in devices could assert a *contributory infringement* claim[14].

---

[10] RAUBENHEIMER, op.cit.

[11] See the Belgian Report.

[12] *Sega v. MAPHIA*, (857 F. Supp. 679, 685 (N.D. Cal. 1994)).

[13] *Sony Corporation of America et al. v. Universal City Studios, Inc., et al.*,464 U.S. 417, 104 S. Ct., 774, 78 L. Ed. 2d 574 (1984).

[14]Such a doctrine has been used as a defense in the Napster case.

d. Contract law

Circumvention, manufacturing or trafficking in circumventing devices can in some cases constitute a breach of contract. For instance, license contracts can prohibit the defeating or tampering with a protection or management mechanism embedded in the work. Other types of clauses can be found in the agreements between rightholders, technology providers and consumer electronic or computer industries. Such agreements aim at laying down the conditions to be met by players or other devices incorporating a technical protection scheme. An example is the CSS (technical protection of the DVD) license that prevents the DVD players manufacturing industry from decrypting it[15].

Contract law is a straightforward and obvious protection against anti-circumvention, even though it is limited to the contracting parties. It can be particularly helpful in agreements and trade practices between different industries. National reports do not provide for many examples of such contracts, but the French report mentions that license contracts delivered by collecting societies for on-line exploitation of works require diffusion in streaming. Streaming is not, as such, a technical protection means but it prevents copying the work when it is transmitted.

1.2. The protection of communication networks : Telecommunication law, broadcasting law and legal protection of encrypted services.

a. Introduction

The first networks of the communication and information society have been those of telecommunications and broadcasting. Our search for anti-circumvention protection has naturally found many relevant provisions within the regulatory frameworks that rule such networks. The richness and diversity of such provisions make it difficult to draw a complete overview of them. Besides they are often so entangled that it is not easy to distinguish between protection related to telecommunications, broadcasting on wavelength, cable or satellite.

Our overview will differentiate between telecommunications and broadcasting rules. However, the boundaries of such a distinction are sometimes blurred and will probably become more indistinguishable through convergence in the information society.

b. Unauthorized interception and reception of telecommunication data.

The offence of unlawful interception exists in many countries. In the telecommunication era, it conveys the constitutional principle of the secrecy of the correspondence. Most national reports

[15] M. S. DEAN & B. H.TURNBULL, "Technical protection measures : the intersection of technology, law and commercial practices", *E.I.P.R.*, 2000, n°5, p. 207.

mention such an offence, either under the telecommunication regulatory framework[16], or under the Criminal Code[17].

Intercepting a telecommunication without authorization is an offence common in the legislation of many countries. What differs is additional offences such as the communication of the intercepted data to a third party (Australia), their disclosure (Finland, Belgium, United States, France, Japan), their publication (United States, the Netherlands[18]), their utilization (Australia, Belgium, Finland, France), their recording (Australia, Belgium, the Netherlands), the alteration, suppression or possession of data (Belgium), The installation of a interception device (Belgium, France), or the illegitimate use of a lawful recording (Belgium, France), the fraudulent use of a telecommunication service (UK[19]). The Spanish law expressly mentions the interception of e-mails.

Since the rationale of such protection is to guarantee the secrecy and confidentiality of telecommunications, the interception of the transmitted content is the decisive element for establishing the offence, whatever the communication is encrypted or not. What triggers the prohibition is not the circumvention of a technical fence or protection, save for the Swiss Penal Code that protects only encrypted services.

Besides the act of interception and disclosure of data, that is covered by all the laws, some countries also prohibit the devices enabling such an interception, e.g. the Australian *Crimes Acts* , the US *Electronic Communications Privacy Act*, and the Swiss Criminal Code. These regulations generally forbid the manufacture, offer, sale, possession and trafficking in means or devices aimed at the unlawful interception of telecommunication data. The Canadian Criminal Code also prohibits the possession of means enabling the use of telecommunication facilities or the obtaining of a telecommunication service[20]. Here, as in Swiss regulation, "telecommunication services" has replaced "telecommunication data"[21]. The notion of "services" is used more in the broadcasting law to which we turn now.

---

[16] It is the case in Australia, Belgium, United States, Finland, Japan.

[17] Such as in France, Canada, the Netherlands and Switzerland.

[18] W. GROSHEIDE, "Copyright and technical protections- Dutch report", in *Copyright in cyberespace*, ALAI Study Days, June 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p. 408

[19] The UK report states that an interception is unlawful only if it is carried out by a telecommunication operator. But the fraudulent use and access to a telecommunications services are prohibited as well.

[20] E.FRANCHI et P.E. MOYSE, "Copyright and technical protections- Canadian report", in *Copyright in cyberespace*, ALAI Study Days, June 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p. 376.

[21] This is also the case in the United States, where article 18 U.S.C. 1029 concerning the fraud in access devices prohibits the commercialization and the use of a telecommunication devices modified for the purpose of obtaining a telecommunication service without authorization.

c. The protection of broadcasting

Pay-TV services and programs are legally protected in many countries. Under such legislation, devices that permit descrambling the programs without authorization are prohibited. The distribution and detention of pirate descramblers are forbidden. Some laws also cover the very act of descrambling or decrypting TV signals or the provision to a third party of descrambled programs. In Belgium (Communauté Française) or Japan, only the decryption activities, and not the circumventing devices are covered by the prohibition. Broadcasters may nevertheless avail themselves of unfair competition law so as to enjoin the distribution of decrypting or descrambling tools[22].

Protection usually requires the programs to be provided in exchange of a remuneration. Remuneration of TV programs is therefore the statutory objective of UK, Belgian, French, Japanese and Dutch legislation. But there are many other reasons for broadcasters to encrypt their signals: i.e., limiting their potential audience reduces the royalties they pay to copyright holders[23]. Other legal or economic reasons can induce them to encrypt their programs and, if they are transmitted by satellite, to restrict their diffusion to a national or geographic territory. Australia, Denmark, Finland, Mexico, Switzerland and some US States do not require signals to be encrypted for remuneration reasons. In such legislation, any unauthorized decrypting, descrambling or any unauthorized access (which presupposes a conditional access scheme, whatever it may be) to the programs triggers the prohibition.

Protection is usually found in criminal law, but some national reports mention that civil action is available to the broadcaster whose programs have been unlawfully intercepted. The United Kingdom offers a unique situation in that the protection of encrypted TV-programs belongs to the Copyright Act. Broadcasters in the UK are indeed protected by copyright and not by neighboring rights[24]. I other countries, legislation sometimes entitles any aggrieved person to bring a claim. Therefore a copyright holder or a related rights holder in the scrambled or encrypted programs could qualify[25].

The technique of diffusion does not matter, except in the United States where different federal laws control cable transmission and satellite transmission. Digital broadcasting through the Internet or webcasting are rarely mentioned, as such, in the relevant legal provisions. Nevertheless, the often technology-neutral language therein could normally cover Internet broadcasting as well. Outside of these neutral provisions, information society services are increasingly dealt with in specific regulatory frameworks, such as the European directive on the legal protection of conditional access which we will now examine.

---

[22] Belgian Report.

[23] A. CHAUBEAU, "Le décodage illicite des signaux de télévision cryptée et la protection des auteurs et producteurs d'œuvres audiovisuelles", *Droit d'Auteur,* December 1990, p. 385.

[24] K.J. KOELMAN & N. HELBERGER , "Protection of technological measures", in *Copyright and electronic commerce*, B. HUGENHOLTZ (ed.), Kluwer Law International, Information Law Series 8, 2000, p. 165-227.

[25] as in the Canadian law, see FRANCHI et MOYSE, op.cit., p. 377; or the US Cable Communications Policy Act, see the US report.

d. *The legal protection of conditional access services: the European directive and the Convention of the Council of Europe.*

The market for encrypted services has radically changed in the last years from pay-TV services to a whole range of Internet services. The expansion of available bandwidth and of the number of broadcasting frequencies, digital development and lower costs for encryption have also played a key role. Nowadays many online service providers have recourse to encryption or other conditional access schemes. Examples of such services, whose provision is based on conditional access, are: on line business services, financial or banking services, consultation services, distance education, access to online databases, video or music on demand, newspapers and magazine provision.

This new market and new players belong to an important economic sector of the information society in which the European Union lawmaker took an early interest. In 1996, a Green paper on the legal protection of encrypted services in the Internal Market[26] raised some questions and underlined the discrepancies between the Member States in that field[27]. The directive on the legal protection of services based on, or consisting of, conditional access is the follow-up of this ground working paper. It was finally adopted in 1998[28].

More recently, the Council of Europe has enacted a Convention on conditional access, cast in the same mould as the EU text[29]. Both documents are so similar that, in what follows, the legal protection they grant will be examined without distinguishing one text from another, except when necessary.

The EU Directive and the Council of Europe Convention will likely play a major part in anti-circumvention provisions, since they enact for the first time a broad protection of online services and technical fences around these. They are also particularly relevant for our report since they present a close relationship with copyright-related anti-circumvention provisions. The implications of this link between both fields, though largely overlooked in the early days, are now regularly addressed by legal scholars[30].

---

[26]European Commission , Green Paper on the legal protection of encrypted services in the internal market, 6th of March 1996, COM (96) 76.

[27] N. HELBERGER, "Hacking BskyB: The legal protection of conditional access services under European law", *Entertainment Law Review*, 1999-5, p. 88, available at <http://www.ivir.nl/Publicaties/helberger/HackingBskyB.html>

[28] European Parliament and Council Directive 98/84/CE of 20th November 1998 on the legal protection of services based on, or consisting of, conditional access, O.J. n° L 320, 28/11/1998 p. 0054 – 0057.

[29] European Convention on the legal protection of services based on, or consisting of, conditional access, STE n°178, 24 January 2001.

[30] TH. HEIDE, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", (2000) *B.T.L.J.*, Vol. 15, No. 3, p. 993-1048; K.J. KOELMAN & N. HELBERGER, op.cit.; S. DUSOLLIER, "Incidences et réalités d'un droit de contrôler l'accès en droit européen", in *Copyright : a right to control access to works ?* Cahiers du CRID n°18, Bruylant, , Brussels, 2000, p. 25-52.

The conditional access directive covers radio or television broadcasting services and information society services, normally defined in European Union legislation as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services* "[31].

Protection applies to services on two conditions. The first one is that the service is based on a conditional access, which is defined as *"any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior individual authorisation"*. The directive also covers the provision of conditional access to the above services, considered as a service in its own right. Thus both the service provided upon conditional access and the technique or the service granting such access are concerned.

The second condition is that the purpose of conditional access is to ensure the remuneration of the service. This requirement has given rise to many discussions. Some important players of encrypted or conditional access services elude protection, such as free TV-programs that use encryption to geographically reduce their audience. Nor is the notion of remuneration is clear : could it cover indirect and non-monetary remuneration, e.g. the transfer of any other economic value such as goods or information[32] ?

The technique that conditions access does not matter. Any mechanism for conditional access is covered, and not only encryption that was at the origin of the directive. These mechanisms include: passwords[33], encryption, biometric techniques or any other device for scrambling or identification. This technological neutrality ensures that the text will survive future developments.

As in broadcasting legislation, conditional access regulations are mainly concerned with circumventing devices, rather than with circumvention itself. The act of circumvention is prohibited neither in the European Union Directive nor in the Council of Europe Convention. But the manufacture, import, distribution, sale, rental or possession for commercial purposes, installation,

---

[31] See the Article 1(2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services, OJ L 298, 17. 10. 1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30. 7. 1997, p. 60).<http://europa.eu.int/eur-lex/en/lif/dat/1998/en_398L0048.html>

[32] N. HELBERGER, op.cit.. Such criticism has convinced the European Parliament to commission, through the European Commission, a study on services whose conditional access does not aim at ensuring the remuneration of services and on the need for a legal protection in that case. This study has been carried out by the Institute for Information Law at the University of Amsterdam. See *Study on the use of conditional access systems for reasons other than the protection of remuneration*. available at <http://www.ivir.nl>.

[33] Whether it concerns passwords as well is not certain in the EU directive that forbids illicit devices or software. A password is merely information aimed at obtaining access and should not be covered by the directive, except where national legislators transpose the directive so as to cover passwords as well. It is namely the case in the Dutch Criminal Code that prohibits the use of passwords to receive unauthorized signals using technical means or a false signal. This notion of "device and software" shows that the directive has its roots in the protection of encrypted service. See K.J. KOELMAN & N. HELBERGER, op.cit., p. 47.

maintenance or replacement for commercial purposes of an illicit device and the use of commercial communications to promote illicit devices are prohibited. Illicit devices are defined as "*any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorization of the service provider*".

But providing the decryption key on a website free of charge, like any other non commercial ways of distribution, is not prohibited, which is arguably a great deficiency of protection[34].

Both the directive and the convention state that the remedies should be a matter for each member State. They must at least be effective, dissuasive and proportionate to the potential impact of the infringing activity, which could involve criminal charges.

Legal protection is granted to protected service providers and providers of conditional access services , i.e., the providers of the conditional access technique, who should be able to claim damages and obtain an injunction. Whether the copyright holders in the contents of the protected services could similarly be entitled to bring a suit has been widely discussed in the European Parliament[35]. No such possibility has been accorded, even if it has been stressed that their interests should and will be exclusively taken into account in the anti-circumvention provisions of the copyright directive. Once again the protected interest is emphasized i.e., the remuneration for the service and not its content or value.

All EU member States have not yet transposed the CA directive, even though the deadline to do so was in mid-2000. National reports shows that Denmark, the United Kingdom[36] and Italy have duly complied with their obligation in that matter. Projects for transposition are in progress in Germany, France, Spain and Finland. In this last case, as in the Netherlands, the legal protection of encrypted services already covered information society services.

e. *Pros and cons of protection in broadcasting or conditional access regulation*

Broadcasting or conditional access regulation usually requires that protected services be provided against remuneration. We have seen the criticism generated over this requirement[37]. This requirement also constitutes a real hindrance for copyright holders who would avail themselves of such legislation. Indeed, when access to copyrighted works is technically conditioned, it is not necessarily focused on ensuring the remuneration for the service.

---

[34] N. HELBERGER , op.cit.

[35] The report of the Economy and Social Committee suggested to make the claim available to any concerned person (J.O.C.E., No. C 129, 27.04.1998, p. 16); The Legal Affairs Committee proposed to include explicitly the copyright holders (Rapport A4-0136/98)

[36] The UK case is interesting since it transposes the conditional access directive in the Copyright Act.

[37] A. CHAUBEAU, op.cit., p. 385 who explains why they encrypt their programs in other cases, namely to restrict the audience for technical of economic reasons.

Protection is granted to the broadcaster or, in the conditional access directive, to the protected service provider. The rightholders of the program or of the works contained in the service are not primarily covered[38]. As far as the conditional access scheme is concerned, this point is not so problematic. If the copyright owners communicate their works on the Internet based on conditional access, they could qualify as protected service providers[39]. On the other hand, in most cases of on line exploitation of IPR-protected content, the service provider might be the rightholder, for instance the owner of rights to the database, the producer or the publisher.

1.3. Computer crime law

a. Introduction

Computer crime legislation has blossomed in the last twenty years as a response to the security attacks on computer systems and networks. New offences have been defined within this new field of criminal law, some of them being helpful in anti-circumvention protection.

Some recent international regulations round off the national ones, in attempting to offer a harmonized solution for the many threats to the security of naturally international networks. One draft convention of the Council of Europe on cybercrime[40] could soon become a standard in that field. So we will use it as a reference. It imposes changes and adaptations in criminal procedure and in rules of international cooperation. It also proposes some specific computer-related offences.

b. Hacking and unauthorized access to computer systems

Hacking is a key offence in the Council of Europe draft Convention. "*When committed intentionally, the access to the whole or any part of a computer system without right*" should be established as a criminal offence. What is prohibited is not the defeating of any technical barrier, as in anti-circumvention provisions, even though the Draft convention provides that a country may require that the offence be committed by tampering security measures. However, most existing legislation does not impose such a requirement[41].

---

[38] A. CHAUBEAU, op.cit., p. 388; See the Spanish report that cites a court decision where a person who had transmitted to third parties TV programs decrypted without authorization has been held liable for intellectual property rights infringement.

[39] See for more details on that question, S. DUSOLLIER, op.cit., p.49.

[40] Draft Convention on Cyber-Crime (Version n°27- Revised), available at <http://conventions.coe.int>

[41] S. SCHJOLBERG," The legal framework – Unauthorized access to computer systems, Penal legislation in 37 countries", <http://www.mossbyrett.of.no/info/legal.html>

The article 3 of the draft also makes illegal "*the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*".

A similar condition appears in both offences : the access or interception has to be committed "without right". The explanatory notes clarify this notion by referring to behavior not justified by any legal, administrative, judiciary or contractual power, or to behavior not justified by any established legal exception, excuse, defense or legal principle. The question that arises here is whether access to works and circumvention prior to this access could be justified when the ultimate aim is to exercise copyright exemptions. The answer is not straightforward. First of all, "without right" refers, in our view, to the act of access and not to the eventual activities. What is done with the data to which hacking gave access is not relevant here. What matters is the very act of hacking that, if in any way justified, could be considered as being "with right". Cases where hacking is "with right" are not many and vary from a country to another. It could be for instance, intrusion needed to investigate offences, to lawfully test the security of the system or for public order or security.

As far as copyright is concerned, the exercise of an exception should not necessarily legitimate the access to work. Another report will consider this question. This could be the case when the law constrains the author to provide a free access to her work, or at least a unprotected copy thereof, so as to ensure the benefit of exceptions. This may result from the transposition of the article 6 (4) of the European Directive of Copyright in the Information Society of 2001[42]. Should a member State, within the framework of the "appropriate measure" it has to take under article 6 (4), grant a right to some users to obtain a copy of the work without any technical protection measure, bypassing the technical barrier the author would have put around her work might mean that access is not unauthorized under the draft Convention.

Many States already recognize unauthorized access as a criminal offence, a fact that is confirmed by all national reports we receive.

The elements of the offence differ slightly from one country to another. Some States, such as Switzerland, Italy, Norway, Finland or Germany[43], require the computer system to be specially protected for access to be considered as unauthorized. The existence of technical measures will thus be necessary. In other countries, the default of an authorization suffices, even if this default results from technical protection. The US Computer Fraud Act[44] requests , in addition to the access without authorization, the receipt of certain information, its alteration or suppression.

---

[42] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJEC L167 22/06/2001).

[43] S. SCHJOLBERG, op.cit.

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

France, Belgium, the United Kingdom and the United States also punish the unauthorized maintaining in a computer system or the abuse of an access authorization. This could encompass prohibiting the circumvention of technological measures that limit the use of works even though access thereto has been duly authorized by the author. For instance, a video-on-demand service works on a subscription basis when all uses are eventually invoiced. A user manages to disable the technical system that monitors uses and delivers the invoices. The offence of unauthorized maintaining could cover the uses of the system as enabled by the circumvention, thereby exceeding the access granted by the author. Going beyond the number of legitimate users or bypassing pay-per-view or pay-per-time monitoring systems could be other examples[45].

Using, altering, damaging or suppressing data or information obtained through hacking often constitutes aggravating circumstances. The Belgian report says : "*reproducing or communicating to the public the date and works to which the hacker has had access, using elements of a software whose reverse engineering has circumvented protection measures or making use of databases or the computer systems once the technical fences have been bypassed, will be circumstances that will aggravate the penalty for hacking*". Deleting elements of the technical protection process or manipulating this process so as to disable it will lead to the same result.

c. Hacker tools

Up to a few years ago, hacking was a solo race, where competitors were mostly trying to outmatch their rivals. It has recently become a team sport whose members share tricks and tools, particularly with the development of the digital networks.

On that basis, recent computer crime laws add the prohibition of tools enabling or facilitating hacking activity to the offence of unauthorized access. These are called "hacker tools". They include decryption keys, software enabling to 'crack' access codes or any other security systems, passwords, etc. The article 6 of the draft convention of the Council of Europe lays down:

> *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
>
> > *a) the production, sale, procurement for use, import, distribution or otherwise making available of:*
> >
> > > *1) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;*
> > >
> > > *2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed*

[45]See the Belgian report.

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches»

The Swiss, Belgian, Italian and Greek reports mention a prohibition of hacker tools. The US report cites two pieces of legislation, one dealing with trafficking in passwords, the other relating to the fraud in access devices. Passwords are also protected in the Japanese criminal Code. In France, the hacker tools are not in themselves prohibited but, as the French report states, people offering or selling such tools could be sued as accomplices.

d. Other computer-related offences

National reports mention other offences that could make circumvention liable to prosecution.

Computer fraud appears in the Belgian, United States, Finnish, Spanish, Greek, Swiss[46] and Danish reports. The Council of Europe defines computer fraud as *"the causing of a loss of property to another by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer or system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another".*

This offence could apply to certain acts of circumventing technical protection measures such as the introduction of license numbers found on the Internet in a pirated computer program, the introduction of a decryption key or software circumventing the protection. The economic benefit, gained without right, would be the use and the copy of a work without the authorization of the copyright holder.

According to national reports, other relevant offences could be the alteration or the damage to data in Switzerland, Spain, Germany or Mexico, the fraudulent use of a computer in Swiss and Spanish laws, the unauthorized reception of data or the sabotage of data processing in German law, the forgery or the modification of computer material in UK law.

e. Pros and cons of protection by computer crime laws

Cybercrime-related provisions could help incriminate numerous forms of circumvention. The unauthorized access offence, as it is broadly construed in most legislation, could be applied, except for one difficulty: a copy of a work may not be easily considered like a computer system, which is normally the target of the intrusion in order for the offence to be established[47]. Unauthorized access to

[46] The Swiss criminal law tells about receiving a service by fraud.

[47] K.J. KOELMAN & N. HELBERGER, op.cit., p. 35

a work would thereby qualify as a crime only if criminal law covers both access to the system and to the data that it contains and processes. This is the case in some recent laws.

Another solution would be to consider a collection of works available online (e.g. videos on-demand) as a computer system. It would be easier to prosecute the act of hacking on a website hosted by a server, qualified as a computer system, that enables access to or copy of the work without authorization[48].

The crime of hacking is not likely to cover access controls that are installed at the level of the user, such as the decrypting of the work carried out by a software application embedded in the computer or player device. If the user employs a decrypting key she found on a hackers' website so as to decrypt and play video-games or DVD she has lawfully acquired, such an access on her own computer system can not be considered an unauthorized access felony.

Recourse to criminal law presents other two main disadvantages. First, criminal procedure is often cumbersome and takes longer[49]. Second, criminal provisions are to be strictly construed. This implies that if a circumvention does not exactly fit the wording of the felony, it will not be prosecuted on that basis.

1.4. Intellectual property rights in the technical measure

a. Introduction

Circumventing or defeating a technical device is likely to mean manipulating it in such a way that it could infringe rights to the technique itself. This brings us closer to intellectual property rights. Copyright, patents, protection of know-how and secrets could be areas where useful anti-circumvention protection can be found. Some case law confirms it.

b. Copyright in the software

When the technical protection measure that prevents copying, accessing the work or ensures its authentication, is a computer program, hacking it could constitute an infringement of the copyright vested in the software. Tampering with the protective mechanism could arguably imply a reproduction, even if transient, of the software[50].

---

[48] See the Dutch report.

[49] See the UK report.

[50] This implies that the act of reproduction, where it is only temporary, falls under the monopoly of the author. On that point, see Y. GENDREAU ," The reproduction right and the Internet", *R.I.D.A.*, October 1999, n°178, p. 2-81

Such reproduction will be likely when developing a circumventing, defeating or emulating device[51]. The first stage in the conception of this anti-protection will aim at understanding its operation. Eventually, the system will be tested several times. The hacker will usually make a complete copy of the program to be able to study it thoroughly[52]. Reverse engineering, testing and making a copy of the program are reproductions, whether permanent or temporary, that need to be authorized by the right holder, who could sue for copyright infringement against developers of circumventing tools. Persons who traffic in such tools could avoid such a lawsuit since a commercialization of anti-software does not amount to a reproduction of the program..

The use of circumvention tools could also constitute a copyright infringement of the protection software if they imply the reproduction of its elements.

National reports mention some case law on that basis. In Germany several judgements held that circumventing security software entails its alteration, thereby infringing the adaptation rights of the software author[53]. An Australian court found that the operation of a dongle (i.e. a verification routine granting access to the software by legitimate users) was a substantial part of the protected software. Disabling it means reproducing it. Here the technical measure is not considered as an independent software but in its interaction with the work it protects. Thus the technical protection measure and its object are merged.

Another Australian decision has admitted the protection of the protection device as a computer program on condition that it is original. Another question in that decision was to determine as to whether the data processed by the verification routine are a protected compilation under Australian copyright Act[54].

In the United States, prior to the DMCA, the developer of a software-based copy-protection system sued a competitor who offered a program that managed to undo that protection system[55]. The plaintiff, Vault Corp., argued that by testing and reverse engineering its software, the defendant, Quaid Software Inc. had infringed its copyright. It also contended an infringement of its right to make a derivative work of its own software. The court rejected both contentions on one reason : the circumventing program, developed by Quaid, was also capable of legitimate uses, such as the making

---

[51] For instance, the emulators that simulate the operation of software that aims to authenticate the exemplar as an original.

[52] X. LINANT DE BELLEFONDS, obs. sous Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

[53] See J. KAESTNER," Law and technology convergence: copyright", in I. WALDEN & J. HÖRNLE (ed.), *E-commerce law and practice in Europe*, ECLIP Publication, Woodhead Publishing, 2001, Chap. 2, p. 8, and the mentioned case law.; A. RAUBENHEIMER, op.cit.

[54] See the Australian report.

[55] *Vault Corp. v. Quaid Software*, Inc., 655 F. Supp. 750 (E.D. la. 19870, aff'd, 847 F.2d 255 (5th Cir. 1988).

of a back-up copy of the technically protected software. Besides, specific acts of testing and reverse engineering in which Quaid engaged to develop its bypassing device, were authorized by the license[56].

This US case is a good illustration of the limitations on protection against anti-circumvention by copyright in software. Other decisions had to rule on similar issues. In France[57] a defendant argued that the circumvention of a software-based copy-protection aimed at making a back-up copy. Nevertheless, French case law narrowly construes the back-up copy provision in the copyright law. Such a copy is authorized only if the software producer has not provided the user with one back-up. Besides, it is worth noting that under French law, making this copy is not a right granted to the user, which means, that the copy can not thwart a copy-protection mechanism even though the judge has not expressly said so [58].

Copyright exception for reverse engineering is also frequently argued in such cases, without great success. To be exempted from copyright, the purpose of the decompilation must be the development of an interoperable software. In cases where reverse engineering aims at developing a circumventing program, such decompilation could not be considered as a legitimate exception to copyright[59].

The Belgian report adds that one flaw in this protection regime is that only the holder of copyright in the protective software could claim infringement and not the owner of rights to the protected content. Anyway, some remedies in copyright laws benefit any concerned or aggrieved person, including the copyright holder using the software-based protection[60].

c. *Patent law*

The technical process embedded in the measure can be patented. The patentability of software should no longer be an issue. Nevertheless, patent protection is not a very relevant anti-circumvention provision. Firstly, patent confers an exclusive right to manufacture, use, sell and place on the market the subject matter of the patent.[61]. With regard to process patents, the rights granted differ from country to country ranging from similar exclusive rights in the product made according to such process down to no rights at all.

---

[56] P. SAMUELSON, "Intellectual property and the digital economy: why the anti-circumvention regulations need to be revised", *Berkeley Technology Law Journal*, Vol. 14:1 (1999).

[57] Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

[58] X. LINANT DE BELLEFONDS, op.cit..

[59] see, concerning copyright-related anti-circumvention provisions, *Universal City Studios, Inc. v. Reimerdes*, 2000 WL 48514 *2 (S.D.N.Y. 2000); JANE C.GINSBURG, "Copyright use and excuse on the Internet", 24 *Columbia-VLA J.L. & the Arts*, 2000.

[60] See the Belgian report.

[61] S. LADAS, *Patents, Trademarks and Related Rights : National and International Protection*, Harvard University Press, Cambridge, 1975, T. I, p. 396, § 232A.

Circumventing a technical measure or selling circumventing devices will not amount to the manufacture or sale of the patented product or process. Maybe the circumvention will aim at manufacturing products according to the patented process. In this case, this manufacturing, and not the circumvention, will constitute an infringement of the patent rights. In general, circumventing devices do not reproduce the technical process but defeat it.

d. *Trade secret and know-how*

Disclosure of trade or business secrets is prohibited in many countries through different legal techniques: the law makes it a felony, an unfair competition practice, or the protection is granted in labor law.

The TRIPS agreements recommend adoption of rules in unfair competition law that would protect undisclosed information so long as such information is *"secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; has commercial value because it is secret; and has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."*[62]. Accordingly, persons should have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices.

As far as we know, at least one case has used trade secret in an anti-circumvention litigation. It was the first episode of the famous serial that dealt with the DVD decryption. Before a Californian Court, the DVD-protection association sued websites disclosing information for decrypting the DVD.[63] The Court considered the encryption key as a protected trade secret, even though decrypting it was possible. The economic value of the DVD is actually related to the encryption process. For the disclosure to be unlawful, information should have been obtained in an illegitimate way. The Court held that reverse engineering the protection process in order to obtain information necessary to make the decryption method was illegitimate, since the license of the product forbade it. .

Consequently, disclosure of secret information related to a method of technical protection would infringe trade secret regulations[64]. This ruling is nevertheless limited to the disclosure and does not concern the circumvention in itself, the manufacture or the sale of devices based on such information.

---

[62] Article 39 §2 TRIPS.

[63] *DVD Copy Control Association, Inc. v. Andrew Thomas McLaughlin et al.*CV-786804 (Ca. Super. Ct filed Dec. 28, 1999

[64] A. RAUBENHEIMER, "The new copyright provisions for the protection of computer programs in Germany", *Law, Computers & Artificial Intelligence,* Vol. 4, No.1, 1995, p.18.

Know-how is composed of technical information that is waivable, not available to the public and not patented[65]. Know-how usually benefits from contractual protection. In this framework, disclosure of information about protection techniques could constitute a breach of the know-how contract[66]. Contractual liability has been addressed above.

1.5. Comparison between the different protection regimes

a. The conditions of the copyright-related anti-circumvention provisions

The other sessions of this ALAI Congress will surely emphasize the disparities of the copyright-related anti-circumvention provisions from one country to another. These disparities make it more difficult to determine a common ground on which we could compare anti-circumvention provisions outside copyright. The WIPO Treaties could be the lowest common denominator, but that would offer minimal protection, in which the comparison could be misguided, since the Treaties only prohibit the act of circumvention and not devices.

We could nevertheless take for granted that most anti-circumvention provisions concern both the act and the devices, as it was intended in the Basic Proposals for the Diplomatic Conference of 1996[67]. We will thus examine in each protection regime whether the circumvention act and /or the devices are addressed.

With regard to the subject-matter of the protection, copyright-related provisions cover any technical measures so long they are used by authors in connection with the exercise of their rights. A whole range of technological protection mechanisms has been protected, such as:

- anti-copy protection;
- access control systems, including passwords, hardware or software process, décryption keys;
- authentication routines and codes[68];
- watermarking or any other technique embedding information or stamps in the digital code of the work;

---

[65] M. BUYDENS, *Le droit des brevets d'invention*, Larcier, Brussels, 1999, p. 291.

[66] K.J. KOELMAN & N. HELBERGER, op.cit., p. 36

[67] This is only a working hypothesis. The opportunity to cover both act and devices and to what extent the States protect both could be discussed.

[68] Such authentication processes have been the objet of most US cases under the DMCA. Such technical measures are namely used in DVD or in Realmedia formats, as in video games. Its principle is that the player reads the contents only if it is an original copy and not a pirate copy. Such process also enables a regional coding as in the DVD.

- encryption of the work when transmitted online;
- rights management or usage monitoring tools.

The question we will address is whether the anti-circumvention provisions outside copyright cover so broad a range of technical tools.

Finally, the third point for comparison will be the remedies and actions on which the efficiency of the protection mostly relies.

b. Circumvention act or device

For many people and copyright holders, the real threat to works and technical protection measures lies more in the traffic of circumventing devices, hacker tools, decryption keys and passwords than in the act of circumvention. Yet, the WIPO Treaties, failing a consensus on the Basic Proposal, deal only with the very act of circumvention. Some legal techniques we have addressed follow the same line by prohibiting the circumvention of a protecting device or the bypassing of a technical fence. In such instances, not all regimes refer to the word "circumvention". Some provisions use "interference", "decryption", "descrambling", "breaking", "countermeasure" or "removal". All these wordings infer the existence of a fence between the content and the user. The moment when the user meets the barrier constitutes the key element of the prohibition[69]. What matters in such provisions is the method by which the user gets access to the enclosed data or information.

Conversely, other provisions evolve around unauthorized access to the information or the content, whether a technical fence has been transgressed or not, whether content is technically protected or not. Thus, the prohibition goes far beyond the circumvention[70]. The wording here refers to interception, reception or access.

We come now to the comparison of the anti-circumvention provisions around this criteria of act/device. Defeating a technological measure may be considered, within the limits we stressed, as a fault or negligence and impose liability on the circumventer. The person who develops and commercializes circumventing devices would also be directly or contributorily liable.

Unfair competition law only prohibits trafficking, in the course of business, in devices disabling a competitor's products.

Protection found in network regulations primarily concerns the unauthorized interception of communications. Some laws equally cover any unauthorized reception of a signal or data through telecommunication infrastructure or through broadcasting. Sometimes signals are required to be encrypted or to be provided against remuneration. Sometimes, and it is usual in broadcasting law, the

---

[69] G.T. WILLIAMSON, "Domestic provisions analogous to the anti-circumvention provisions of the DMCA", Draft, 2000, p. 17

[70] ibidem.

protection is twofold and deals both with the act of circumvention/reception and with the distribution of circumventing devices. In some laws, only the distribution of devices is prohibited, such as in the European conditional access directive and convention, wherein only the devices disabling access controls are regulated.

In computer crime, new felonies cope with unauthorized access, defeating computer systems or manipulating computer data. Violation of security measures is increasingly unnecessary as an element of the offence, but the existence of such measures will help prove the lack of any authorization.

Cyber-crime legislation therefore deals more with the act of circumvention than with devices. Nevertheless, recent laws and the draft convention of the Council of Europe evoke the prohibition of hacker tools which could comprise a number of devices enabling circumvention of a protection measure.

Circumventing or developing an anti-measure entailing a reproduction of software-based technical protection could be considered as copyright infringement of the software. The sale or placing on the market and the utilization of the anti-measures will not be treated. Protection by trade secrets or know-how will lead to the prohibition of the disclosure of information embedded in the technical process but not more.

The following comparison table may be drawn[71]:

	Circumvention	Interception/ access	Devices
Liability and Tort Law	X	X	X
Unfair Competition			X
Computer Crime	(X)	X	(X)
Interception of telecommunications		X	
Broadcasting Law	(X)	(X)	X
EU Directive on conditional access			X
Copyright in the software			X (conception)
Trade Secret			X (disclosure)

[71] A cross in the table means that this is the case in most countries. A cross between brackets indicates that it is possible in some countries.

c. *Protected technological measures*

Anti-copy protection should not easily qualify as computer programs for they often consist of signals or codes embedded into the work medium acknowledged by the player device. But disabling or making tools facilitating such disabling could make liable the perpetrators. If the distribution of tools takes place in the course of business, unfair competition rules could also play a role.

Telecommunications or broadcasting laws will not be very helpful except if the anti-copy mechanism operates when the work is transmitted over networks. Nor will conditional access schemes be effective. Systems that prevent copying the work can not be deemed as conditional access technique. Anti-copy protection will operate after access to works has been ensured. Besides, since anti-copy protected contents are generally available to the public, copying should not be considered as illicit interception.

Manipulation of the mechanism is computer fraud where the unearned economic benefit is the copy obtained without any right. Conversely, defeating the anti-copy system would not be considered an unauthorized access or hacking into a computer system, nor a unauthorized use of a computer.

With regard to access control systems, many legal regimes could prevent their circumvention, such as conditional access regulations, of course, but also liability, tort law and unfair competition, protection of TV or encrypted signals where applicable, or many computer crime offences. For instance, inserting passwords or serial numbers unlawfully found on the Internet to bypass the access control is a computer fraud. If the access control occurs prior to the transmission of data, circumventing it could be considered as an interception of telecommunications.

In many instances, access controls are passwords, codes or encryption keys and not software. An exception is the dongle which is a verification routine that has been considered as a computer program in many courts. When circumvention requires its alteration or reverse engineering, protection by copyright infringement in the software-based access control is possible[72]. It is also the case for the computer routine that verifies the proper insertion of the access key in the hardware before running the program[73].

Access codes or processes are naturally secrets and could be protected as such. Furthermore, some countries have specific offences for trafficking in passwords.

Other protection techniques consist of embedding in the works signals or data to be acknowledged, as such, by the player device. Such authentication prevents counterfeited works from being played. Recent US case law held that such mechanisms enjoyed protection under the DMCA anti-circumvention provisions. Protection is not so easy to find in other regimes, save for tort law and

---

[72] J. KAESTNER, op.cit., p. 6.

[73] Ibidem, p. 7 and the case law mentioned in notes 25 to 27.

unfair competition within their strict limits. Such authentication process, which US case law called a "secret handshake"[74], is neither a software nor a conditional access system. Indeed, through the technical measure the access is granted to the playability of the medium of the work, but not to a service provided at distance. Besides, such access does not directly ensure the remuneration, that is required by the conditional access directive, but only prevents piracy. Inserting a pirate disc or video into a proprietary platform could not be considered as an unauthorized access to or an unauthorized use of a computer system.

Watermarking aims at embedding in the work some hidden and indelible information about the work, its author or the conditions for utilization. It is not a software or a conditional access system. Neither protection regimes will apply then. In some countries, the offence of alteration or suppression of computer data could sanction any deletion of watermarked information. If the hacker tries to disable the software that controls extracting and analyzing of watermarked information (e.g. for detecting any infringement), it could be considered as an alteration or a reverse engineering of this program[75].

When the work is transmitted on line in an encrypted form, decrypting it without authorization is punishable under telecommunications law for data interception, computer crime laws for unauthorized access, computer fraud or alteration of computer data, under broadcasting laws, if the transmission is made through broadcast, and under conditional access schemes. The distribution or disclosure of decryption keys could be an unfair commercial practice or an infringement of the secret.

The last technological measure we should address is usage monitoring and right management systems. Their disabling amounts to an offence of deletion of computer data or of computer fraud. In Belgium and France the offence of unauthorized maintaining in a computer system, subsequent to a legitimate access, could also cover such circumvention. In another context, a French court[76] has condemned, on that basis, persons who were lawfully connected to a telematic system where gifts were offered when playing certain games. The duration of the games determined the number of tokens eligible for receiving the gifts. If the user did not play the game, he was automatically disconnected. The condemned people used a mechanism for refreshing the game screen that prevented disconnection and thereby earned more tokens. Such logic is pretty similar to a circumvention subsequent to a legitimate access.

Monitoring systems are generally software whose circumvention could infringe copyright.

---

[74] JANE C.GINSBURG, "Copyright use and excuse on the Internet", 24 *Columbia-VLA J.L. & the Arts*, 2000.

[75] J. KAESTNER , op.cit., p. 26.

[76] Trib. Corr. Paris, 5 November 1996, *Expertises*, n° 202, fév. 1997, p. 81.

	Anti-copy	Access Control	Authenti-cation	Watermar-king	Encryption	Monitoring
Tort Law	X	X	X	X	X	X
Unfair Competition	X	X	X	X	X	X
Unauthorized access		X			X	
Unauthorized maintaining		X				X
Computer Fraud	X	X			X	X
Suppression of computer data	X		X	X	X	X
Interception of telecommunication data					X	
Broadcasting Law		X			X	
Conditional access Directive		X				
Copyright in software		(X)	X			X
Trade Secret		X			X	

d. *Remedies and persons entitled to make a claim*

Most of the legislation we addressed is criminal law. Intercepting data, accessing a computer system, manipulating or suppressing computer data, decrypting a broadcast signal, offering devices enabling to defeat a conditional access system are all usually punishable under criminal law, and sentenced with a fine and imprisonment.

This assumes an important deterrent effect. But the criminal proceedings are also often slower and more burdensome. In circumvention cases, the author is primarily concerned to rapidly stop the circumvention activities, particularly when a market for illicit devices is developing or their diffusion is spreading over the Internet. Therefore, the main issue is to allow the rightholders to bring an action for damages and to obtain an injunction or other preventive measure that meets the need for urgency.

National reports have not provided us with enough information to make a comprehensive comparison on that point. An injunction that could result in the elimination of circumventing devices seems to be possible under unfair competition, broadcasting or conditional access law, copyright in software, as in trade secrets protection.

As to whether the author is entitled to bring a claim against circumvention under regimes outside copyright, it is certainly admissible under unfair competition law or tort law. Some broadcasting laws grant remedies only to the broadcaster. Remedies in conditional access legislation are similarly offered to the service provider. We have seen that this should not preclude holder of rights in the contents.

In two cases, protection mainly benefits the provider of the technological measure and not the author of technically protected works: copyright in the software-based protection and trade secrets. In the first case only the copyright holder of the circumvented software could claim copyright infringement. In the other case, only the persons having secret information under their control can enjoin its disclosure.

2. AN ADEQUATE PROTECTION OF TECHNICAL MEASURES

2.1. The role of anti-circumvention provisions outside of copyright : a leading or a supporting part ?

The comparison of anti-circumvention legal techniques outside the copyright arena shows a kaleidoscopic view, which the Australian report qualifies as a complex patchwork of laws whose protection is certainly not comprehensive.

Yet, alternative regimes might be of some help to the authors in anti-circumvention cases on two levels. First they can fill the gaps in the protection of technological measures in copyright provisions. Some extra-copyright regimes could enable the author to sue the act of circumvention where the copyright provisions only deal with devices[77], or prevent the circumvention technological measures that would not be protected under the copyright regime.

In such instances, computer crime, telecommunications, broadcasting, conditional access and trade secret law could certainly be profitable adjuncts to copyright-related anti-circumvention provisions. Comparison tables we have drawn may highlight, when placed beside copyright provisions, where these alternative tools could help resolve some deficiencies.

Second, provisions outside copyright could play a bigger part on the anti-circumvention scene. Countries could indeed decide to implement the WIPO Treaties obligations on technological measures

[77] The Australian report stresses the usefulness of alternative regimes in that case.

in fields of law other than in copyright,[78] e.g., in conditional access regimes, unfair competition laws or computer crime regulatory framework. The 1996 Treaties do not forbid it[79]. What WIPO requires is only that the protection be adequate.

The WIPO Treaties contracting Party has hence several options. It could transpose articles 11 WCT and 18 WPPT in the copyright legislation, as it is usually done by most countries. But anti-circumvention provisions could find their place in another legal field, whether they concern technological measures aimed at protecting copyright or more generally at guaranteeing the security of any technical barrier or prevention. Here transposition could be exclusively done in one legal field or be shared amongst two or more regimes. In the last case, both protections can be cumulative or complementary. Japan, for instance, separates anti-circumvention of technical measures protecting rights of the authors, laid down in the copyright act, from anti-circumvention of access controls that it regulates under unfair competition law. Different legal techniques respond to two different protection features.

Legislators could also state that their regulatory framework already offers adequate protection to technological measures, in or outside copyright. France had done so when implementing the 1991 software directive to justify the lack of a specific provision related to anti-circumvention devices, save for a peculiar publicity obligation[80]. It had been asserted that the general regime of aiding and abetting copyright infringement could sufficiently cover the prohibition of circumventing devices according to confirmed case law[81].

The EU directive on copyright in the information society gives to Member States the same freedom of transposition, while only requiring , as in WIPO Treaties, that protection be adequate and that the remedies be effective. In our view, nothing induces a mandatory transposition in copyright. However, the easily-overlooked article 8 of the directive limits this freedom. IT lays down that each Member State shall take the measures necessary to ensure that rightholders can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of circumventing devices. The legal field in which the anti-circumvention provisions will be placed should therefore include such remedies and sanctions. For example, this will not be the case for computer crime legislation.

---

[78] Opponents to the anti-circumvention provisions in copyright have sometimes argued that new protection was useless since other existing regimes could offer sufficient protection and meet the concern of right holders. According to scholars, the adequate protection was to be found in computer crime, unfair competition law or European conditional access protection. See M.LEDGER & J.P. TRIAILLE, "Copyright and technical protections-Belgian report", in *Copyright in cyberespace*, ALAI Study Days, June 1996, Amsterdam, p. 12,. That text has not been included in the proceedings of the Study Days; W. GROSHEIDE, op.cit., p. 403; K.J. KOELMAN & N. HELBERGER, op.cit., p. 222.

[79] Intervention of KURT KEMPER, Workshop on the WIPO Treaties, 6-7 December 1999, Geneva.

[80] A. LUCAS, *Droit d'auteur et Numérique*, Droit@Litec, Paris, 1999, p. 269.

[81] Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

2.2. The standards of adequate protection

a. The rationale of the protection

Legal regimes outside copyright law have quite different policy objectives that justify the rationale, scope of application and boundaries of each protection. This could be one of the main and irreconcilable differences with copyright-related anti-circumvention provisions that aim, on the contrary, at enhancing the protection of works and authors in a very broad way. Therefore, assessing the adequacy of anti-circumvention provisions on the sole standard of the struggle against piracy and counterfeit would necessarily entail protection in the copyright regimes. Nevertheless, the statutory objectives of other regimes also fulfil some concerns of the authors as far as technological protection is concerned.

The criminal repression of computer hacking has as its main objective to ensure the security of networks and computer systems to which technical fences, whatever they protect, belong. Any activities that undermine this ideal of security are logically prosecuted.

Protecting telecommunications data aims at guaranteeing the privacy, security and confidentiality of communications. This explains why only the act of intercepting the information is prohibited and not the possible breach of a technical defense.

The mission of broadcasting law and recent conditional access legal texts is to ensure the remuneration of radio, television or information society services, thereby protecting the economic interests of the providers of such services. This concern is very close to that of copyright or related rights holders regarding the distribution of their works.

Principles in unfair competition law or in the US Supreme court standard of "*staple items of commerce"* settle conflicts between parallel business activities so as to achieve a fair competitive market. Applying technical fences around products can be considered here as a mere exercise of the freedom of trade. As a principle it cannot inhibit the same freedom of other economic players, except in abusive cases of exercising the latter freedom. This explains why unfair competition law is limited to the prohibition of circumvention activities carried out in the course of a business and offers generally rapid action and recourse.

Some of these objectives could also satisfy the concerns of copyright protection and hence justify the insertion of anti-circumvention provisions in these regimes, totally or partially.

b. The definition of technical measures to be protected.

WIPO Treaties ask for a protection 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". Only technical devices that enhance the efficiency of the rights granted by copyright or related rights are thus concerned. Yet, most transpositions of this obligation go far beyond and comprise as well any technical measures that control access to works or any other technique that has not as its primary purpose the prevention of infringement to reproduction right, communication right or any other rights enjoyed by the author or related right holder. Some of these techniques have been addressed above. One key question is to assess the adequacy of such scope for application in terms of types of protected tools. The response the policymaker will give could preclude some regimes from possibilities for transposition. Indeed, regimes other than copyright could cover some specific techniques, as encryption, or some technical functions, such as access controls that may be considered as being outside the scope of an adequate protection.

Two questions should be asked. First which mechanisms and functions deserve protection against circumvention ? Second, would the choice for anti-circumvention provisions favor an extra-copyright regime, does such a regime cover such key technical mechanisms?

The task will not be easy. It is clear from a look at the comparative table we have drawn of that criteria. Different technical measures are not granted a very comprehensive coverage outside of copyright anti-circumvention provisions.

Anyway, the choice of technical systems deserving protection could entail a distributive legal cover. For instance, rights-technical measures could belong to the copyright scheme, while access controls would better fit in another framework. The main advantage would be to leave out the intricate question of controlling access to works, which is the subject of another report.

c. The scope of the protection: act or device

National approaches are far from converging on that point. Some, such as Australia, prohibit only devices. Japan forbids the act of circumvention only when carried out for a commercial purpose[82]. Others cover both act and devices. There is no common understanding as to whether an adequate protection should cover act, device or both. A decision on that point could of course tip the scale in favor of one regime or another.

d. Adequate boundaries to protection

The adequacy of anti-circumvention protection should take into account the need for defining its own limits. "Adequacy" is not neutral for that matter. It is not only about effective and broad protection, but also about protection that respects the philosophy and balance of copyright, even though the protection

[82] TERUO DOI, "WIPO Copyright Treaty and Japanese Copyright Law: A comparative analysis", *R.I.D.A.*, n°186, October 2000, p. 203.

could be found in another framework. Preparatory documents for both WIPO Treaties and EU directive state that anti-circumvention provisions and remedies should be proportionate.

A consequence thereof is the proper consideration of boundaries to anti-circumvention protection. It is a key but tricky issue. The matter is already extremely sensitive when anti-circumvention provisions belong to the copyright frame. It could be even more sensitive when other legal fields are assessed. A more intricate question is whether copyright exceptions or fair use could be argued as defenses against anti-circumvention prohibitions based on other rights or obligations than those laid down in copyright.

Thomas Heide[83] claims that copyright exceptions, when they are of a binding nature such as in some EU directives, should prevail over any contractual scheme, even outside copyright. The example he provides is a conditional access contractual scenario. It is not so clear that a mandatory exception could prevail over a technical measure, let alone over anti-circumvention provisions outside copyright, unless one argues for the limitations of other rights by copyright exceptions[84].

Copyright exceptions are not stand-alone provisions. They are major parts of copyright law, but they can not be dissociated from the rights and the rationale of the protection. They could not hence be transposed, as such, in other legal fields where objectives are rather different.

Cyber-crime law ensures the security of networks and computer systems. Copyright exemptions do not belong thereto. What matters is the preservation of the technical fence, whatever the purpose for its violation might be. This statement should however be qualified: the intentional or fraud element of the infraction could take into account the purpose to which the circumvention or the unauthorized access has been carried out.

With regard to encrypted or conditional access services, the objective is to protect the remuneration of the service. Here the copyright exception should not intervene for it normally applies once the access to work has been granted.

Prohibiting circumvention devices under unfair competition law could more easily allow for some copyright exceptions, since the rationale is to regulate competitive activities. This concern is close to that of certain copyright exceptions, such as the reverse engineering, that aims at preserving competitive practices[85]. Such exceptions could dismiss an action under unfair competition since they justify the fairness of the activity.

The latter example illustrates that copyright exceptions are not, as such, transposed to other spheres. It is rather the justification underlying them that is admitted in other fields. Freedom of expression, of

---

[83] TH. HEIDE," The approach to innovation under the proposed copyright directive: Time for mandatory exceptions ?", [2000] *I.P.Q.*, No 3, p. 228

[84] For an example in conditional access, see TH. HEIDE, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", (2000) *B.T.L.J.*, Vol. 15, No. 3, p.1046.

[85] TH. HEIDE, "The approach to innovation …" , op.cit.

receiving information, of trade might allow similar or parallel defenses either against copyright suit or other legal suits in circumvention cases.

In some European countries, the fundamental right to receive information underlies the exception of news reporting in copyright and the provisions in the Television Without Frontiers Directive[86], imposing a free access to events of major importance[87]. In the United States, the First Amendment underlies many defenses in anti-circumvention suits, both based on the DMCA or on other regimes.

Such instances where a fundamental freedom could justify a circumvention activity will be rare. In the Netherlands, the *Hoge Raad* rejected the contention of the freedom to receive information, and here to receive encrypted TV programs, justifying the publishing of information about do-it-yourself descramblers[88].

Consequently, appropriate boundaries to anti-circumvention provisions, including fundamental grounds which underlie some key copyright exceptions, should be considered for the adequacy of the chosen legal technique. Opting for a regime with no or few limitations, resulting from fundamental freedoms, public interest or copyright exceptions, is a decisive political choice. The Australian report stresses the threat of an unlimited protection outside copyright. Conversely, in the French report , this threat is seen rather as an opportunity for the authors who could avail themselves of such legal regimes in anti-circumvention cases, without the risk of being baffled by a copyright exception[89]. These contradictory viewpoints urge the need for a reflection on that issue, generally avoided outside of the copyright arena. The enactment of the conditional access directive is an obvious example. Exceptions and limitations or the overall risk of technically locked-in works, information or public domain through anti-circumvention provisions, have been overlooked compared to the fiery controversies they have raised in the discussions around the copyright directive. Yet, if the protection of a technological measure is likely to face a copyright exception[90], why would not the authors turn to another regime that does not allow for the same limit ?

---

[86] Directive 97/36/CE, 30d June 1997, amending the Council Directive 89/552/CEE on the co-ordination of certain provisions laid down by law, regulation or administrative action in member States concerning the pursuit of television broadcasting activities, O.J. L 298, 17.10.1989., p.60.

[87] N. HELBERGER, op.cit.

[88] W. GROSHEIDE, op.cit., p. 408

[89] See also, A. LUCAS, *Droit d'auteur et Numérique*, Droit@Litec, Paris, 1999, p.274.

[90] In the hypothesis exceptions could justify such a defense, which is not, for example, obvious in the European directive.

3. CONCLUSION

This concludes our survey of anti-circumvention provisions. One outcome could be to restore the adequacy and legitimacy of the copyright regime as far as anti-circumvention provisions are concerned. Indeed, prohibition of circumvention acts or devices are certainly possible in each area we visited, but with great uncertainties and difficulties. The very question of finding anti-circumvention provisions here and there and seeing how they fit into a copyright rationale, is perhaps irrelevant altogether. By availing oneself of tools whose objective and conditions are largely different from copyright concerns, one would only distort and weaken such tools. Not surprisingly, twisting legal principles and notions results in twisted solutions.

Another key issue is the few limitations of extra-copyright anti-circumvention provisions, or at least the little debate in that regard. It is worth saying again that a protection would be adequate and comply with the WIPO requirement only where it shows a fair balance, as in copyright. On that ground, anti-circumvention provisions could more easily find their place in copyright law, where discussions about exceptions versus technological measures have occurred, no matter how satisfactory the outcome is considered to be.

This emphasizes what a key issue the conflict between exceptions and technical fences is. The epicenter of the issue might be in copyright as its tremors should be felt in the other legal fields as well. If exceptions could be excluded by simply turning to another legal anti-circumvention scenario, what would be the point in attempting to legally solve the clash between the interests of society and a technically locked-up world of information ? This is a particularly intricate matter whose consideration outside the copyright regulatory framework may appear to be out-of-place. Yet, if we confuse legal institutions, their boundaries would become entangled as well.

Laying down anti-circumvention provisions in copyright appears then to be a sensible choice. Nevertheless, at the same time it could be decided to limit such a protection to the rights of authors and related rights holders, and to nothing more. Technological measures aiming at another purpose, such as conditioning access to the work, even though they indirectly benefit copyright protection, would consequently belong to legislation more appropriate to meet such concerns.

Anti-circumvention protection could then be moving between copyright and complementary regimes in order to make up possible deficiencies in one protection or another, cover different types of technical measures or entitle other persons than the copyright holder to bring a claim. That could nevertheless not result in an over-protection of technological devices that, at the end of the day, would make them more unpopular than they are today.