Legal issues of electronic rights management systems : COPEARMS ESPRIT project 20460 : deliverable 4.2., 5 octobre 1998

Ledger, Michele; Rolin Jacquemyns, Laetitia; Lardinois, Jean-Christophe; Dusollier, Séverine; Poullet, Yves

Publication date:
1998

Document Version
Publisher's PDF, also known as Version of record

COPEARMS ESPRIT Project 20460

Co-ordinating Project for Electronic Authors Right Management Systems

Legal Issues of Electronic Rights Management Systems

CRID

Deliverable 4.2.

05/10/98

Document Identification

Document ID : ***deliverable-4.2***

Authors : ***CRID : Séverine Dusollier, Michèle Ledger, Rosa Julia, Laetitia Rolin, Jean-Christophe Lardinois, under the supervision of Prof. Yves Poullet ans Séverine Dusollier (the name of the author(s) of each part will be mentioned in the text)***

Date of issue : ***1st October 1998***

Description : ***Legal issues of Electronic Rights Management Systems***

Abstract :

The development of the multimedia technology and of the information superhighways has raised new fears for copyright holders. In the Information Society, it has become easier to reproduce and communicate a protected work without any loss of quality. Facing this threat of a highest level of counterfeiting and piracy, Electronic Rights Management Systems or ERMS provide for a new way of authorising and monitoring uses of protected material on the electronic networks. A prerequisite for such an electronic IPR management is nevertheless to comply with relevant regulations namely related to the legal acceptance and value of digital documents and signature, personal data protection, protection of consumers. On the other hand, the regulatory framework in which the ERMS operates, has to be considered in order to encompass the validity of operations enabled by the technology. The main concern is that the ERMS, which enshrines various licence contracts, encompasses the provisions of IPR requirements, for instance as regards the balance between copyright protection and fair use or copyright exceptions. Finally, the protection of the ERMS itself against any circumvention raises new concerns in the field of the balance between the law and the technology

Warning:

This deliverable consists of a collection of the legal deliverables the CRID has drafted in the course of the COPEARMS project with the addition of some legal issues that have not been addressed at present. Therefore, the titles II.2 (Subject matters of IPR), II.3 (Protection of Databases), IV (Legal acceptance of digital documents and electronic signature), of this final deliverable are resumed from the deliverables D.4.2.1. to D. 4.2.7. The Title II (data protection) has been slightly amended. The other parts of the deliverable were unreleased so far.

Distribution List

Cop	Name	Organisation	Role
	Dominique GONTHIER	CEC/DGIII	ESPRIT Officer
	Dominique SPAEY	BvD	Project Office
	Georges VAN SLYPE	BvD	Project Office
2	Gerard EIZENBERG	CERT	Partner
3	Dominique YON	CISAC	Partner
	Yves POULLET	CRID	Partner
	Rosa JULIA	CRID	Partner
	Jean-Christophe Lardinois	CRID	Partner
	Laetitia Rolin	CRID	Partner
	Jean-Francois BOISSON	EURITIS	Partner
5	Edmond F. KOUKA	EURITIS	Partner
	Graham Peter CORNISH	IFLA	Partner
6	Judy WATKINS	IFLA	Partner
7	Richard CARR	Level-7	Partner

Table of Contents

I. INTRODUCTION

Electronic Rights Management Systems[1] give rise to various legal parameters that must be considered, at the stage of development (such as IPR issues, data protection, secure transactions) and at the stage of deployment (protection of the integrity of ERMS, data protection, consumer protection, ..) of the technical system. The legal constraints that should be taken into account early on are those that will have an incidence on the design of the technology : the technology will have to accommodate the legal requirements and be designed in function thereof. Some of these requirements are very specific to the development of the ERMS and consequently are only just starting to be perceived and analysed. They are nevertheless of fundamental importance to developers since we see them as guiding the way in which the technology should be shaped. One major issue is the risk that the whole system of copyright protection applied to the network will be replaced by a contractual based system on the one hand and that information that has been available freely in the analogue world on the other hand will become wrapped in the ERMS.

On the other hand, those issues that are important when deploying, commercialising or using the technology, are not specific to the ERMS. They are common to any type of service that is offered on the network.

Before considering the legal issues to be taken into account, it is important to recognise that there is no definition accepted at the national or international level of an ERMS. At the IMPRIMATUR Consensus Forum held in London in November 1996, the following definition was suggested:

"An ERMS involves the tagging of works or manifestations of works to enable licensing so that there can be monetary return for use. ERMS must not negate Copyright exceptions"

1 hereinafter ERMS. The transition from Electronic Copyright Management Systems or ECMS to ERMS has been done in the course of the Copearms Project since it has been noticed that the rights monitored by such a technical device were not essentially copyright. Of course neighbouring rights and the sui generis right applied to a database are entitled to be protected and managed by an ERMS. But other content might be protected by the same technology.It might also be mere contractual rights managed by an ERMS between business partners..

The generic CITED ERMS reference model[2] offers the following definition:

> *"An ERMS (Electronic Rights Management Systems) is a software, and possibly a hardware product, associated with one or several copyright applications (such as on-line data bases and CD-ROMS) and aimed at authorising the access to and usage of these applications and managing their IPR (Intellectual property rights)"*

Suffice it to say that an ERMS can perform, any of the following functions[3]:

•<u>According to the terms of the in-built electronic licence agreement</u>,

*monitor the access to and the usage[4] of the *copyright application* by the various agents and prevent the access and use by unauthorised agents and manage the payments received;

•<u>According to the legal environment in which the ERMS is being developed and deployed:</u>

*Supporting security functions such as authentication, data integrity and protection, non repudiation of transactions;

*Ensuring the rights of the users in relation to the exceptions to the exclusive rights of the right holder;

*Ensuring the rights of the consumers are respected

•<u>According to the level of development of the ERMS:</u>

*Preparing invoices to end users and acknowledgement of debts to right holders,

*Integrate EDI messages;

*Integrate work identifiers;

*Enable electronic payments;

*Communicate with other ERMS.

---

2 The COPEARMS ERMS model group. *The CITED ERMS reference model, Volume 1: Electronic Copyright Management: Business Requirements and Design Guidelines (draft 4)* AC664/Deliverable. February 11, 97

3 See COPEARMS ERMS model group. AC664/Deliverable. p. 9

4 Access. search. retrieval. display. print. copyrighted application update operations.

It is important to stress the three following characteristics of ERMS which entails major legal consequences :

- an ERMS registers the terms of contracts between the concerned agents so as to manage the IPR of copyrighted application according to the terms of the contracts. A key principle is that the parties are free to decide on the terms of their contract with the important limitation that the contract may not override binding legal provisions. This priciple shall be of utmost importance as regards for instance the copyright exceptions[5].

- an ERMS is a blind technology which implies that the ERMS as such is not able to check the compliance of its operations with the relevant laws. This means that the ERMS can only detect the technical usage carried out or requested by an user. The design of the technology and the framework of its operation (e.g. contract of use, conditions for user registartion, etc...) has to fill this gap by taking into account the most relevant regulations and embed such compliance in the technology itself.This characteristic is also particularly relevant as regards the copyright exceptions.

- an ERMS is universal and should enable to function through the Information Society in such a way that it complies with relevant legislation throughout the world. As any other Information System, the regulatory framework is therefore a particularly intricate issue.

FOREWORD AND TERMINOLOGY

In this Deliverable, we use the same terminology as that of the COPEARMS Business Model, as regards the agents, the application. The following definitions are resumed from the Business Model :

- A **copyrighted application** is a set of one or more digital intellectual works under copyright or any other related rights (neighbouring rights, sui generis right) or contractual rights and of an associated processing facility (exploitation software and, possibly, hardware)

[5] see below, title II.5

permitting to produce, store, disseminate, use, search, retrieve, display and/or listen to, copy ...the work, or a part thereof. Copyrighted applications could be:

databases: with primary information (full text, with possibly images and sounds in monographs, journals, patents, computer programs, statistics; still or animated images; music,...), secondary information (bibliographic data), tertiary information (directories,...), or with a combination of primary, secondary and/or tertiary information,... with or without value added features such as indexes and cataloguing data, courseware's: non interactive or interactive, with, e.g. exams, automatic marking and corrections,digital audio and video recordings, digital multimedia recordings: interactive or not, with sounds, texts, games, quizzes, still images, animated images, video clips, digital radio and TV broadcasting.

A copyrighted application could be made of a single work or of a composite work or of a set of works; a work could include several work components, possibly divided themselves into several sub-work components.

• A **work component** is a part of a copyrighted work or application that is distinguished from the other work components of the same copyrighted work or application by the fact that:

either it belongs to a different originator or publisher/producer (e.g. the image of a painting, belonging to museum X, in an electronic art book),

or it has different use rights attached to it (e.g. part X of a courseware accessible only by teachers and part Y accessible by students and teachers),

or it has different use right charges associated to it (e.g. an index accessible for free and a bibliographic citation accessible for a fee).

Agents

Originators, also called creators, are authors, writers, teachers, composers, painters, architects, stylists, film and play actors, musicians, singers, dancers, software programmers, etc..

They create intellectual works for usage by other agents.

Publishers/producers are book and journal publishers, compact disc producers, film producers, video producers, radio/TV producers, CD-ROM producers, etc..

They carry out services on the intellectual works by activities such as reviewing, checking, assembling, arranging, completing, customising, verifying, manufacturing,

multiplying, dispatching, etc., and may turn them into copyrighted works or applications. The publishers/producers also define the use rights or privileges (i.e. the usage operations that the concerned agents could be authorised to perform) of the various types of agents liable to access the copyrighted application or work.

Distributors are on-line database host vendors, bookshops, records shops, libraries, INTERNET site providers, broadcasting companies, dealers, retailers, information brokers, universities, etc.

They analyse production, customisation and consumption processes caused or triggered by other agents. They acquire copyrighted works or applications from their publishers/producers (through a distribution or a licence contract that makes them partial right holders of the works, and possibly of their associated exploitation software); they encapsulate the works with a software/hardware device to transform them into copyrighted applications; they distribute them to end-users; their activity leads them to pay royalties to the concerned publishers/producers, originators and/or collecting societies. They may also enrich the copyrighted applications with value added data such as indexes, links with other applications, advertisements,... They define, within the framework of their contract with the publishers/producers, the use rights they allocate to the end-users.

Collecting societies are authors' societies, composers' societies, licensing societies, societies managing the reproduction rights.

They recover royalties for the exercises of representation and reproduction rights of some types of intellectual works such as musical, dramatic, choregraphic and cinematographic ones,

Collective end-users are industries, enterprises, associations, government services, libraries, hospitals, schools, universities, etc.

They obtain the right, through a purchase contract or a utilisation licence concluded with either a distributor or directly with a publisher/producer, to access to and utilise the copyrighted work or application according to the terms of that contract. They pay to the distributor or to the publisher/producer, either a lump sum (use right credit) when acquiring the application or when ordering new use rights, or a utilisation fee (use right charge) after each set of utilisation of the application, or a (reduced) lump sum and a utilisation fee.

Individual end-users are members of a collective end-user organisation: employees, civil servants, teachers/professors/ tutors, students/ trainees/learners, physicians in hospitals, etc.

They are appointed or registered by the collective end-user organisation and receive from it their use rights, within the set of allocable use rights listed in the contract concluded between the collective end-user and the distributor or the publisher/producer of the copyrighted work or application. Within a collective end-user organisation, individual end-

users may belong to different types (according to their occupations, functions,...), each of which liable to have specific use rights (e.g. students and teachers using the same courseware: the students to consult it, and the teachers to update it).

Private end-users are consumers, listeners, readers, spectators, private physicians and lawyers, etc.

They obtain the right to access, and to use the copyrighted work or application by:

* buying a music or video disc or a CD-ROM, in a retailer or a dealer' shop,
* buying a computer program, with its associated licence contract, in a retailer/dealer' shop,
* concluding a contract with a cable radio-TV network operator,
* paying a fee to a pay per view TV operator,
* concluding a contract with an on-line host vendor for a utilisation fee or for free,
* or simply accessing data on an INTERNET site as a shareware to be post-paid in case of actual use, or a "kiosk" application on a national teletex server for a utilisation fee.

In those cases, a part of the utilisation fee will be paid by the distributor either to the publisher/producer or to a national collecting society.

Use rights managers or URM

They are the people or organisations responsible for the customisation, creation and operation of the ERMS: recording the identifiers of the concerned works/applications/work components and of the concerned agents, recording the use right each agent has towards each work/application/work component and the associated business conditions (such as fees), declaring the usage operations to be monitored by the ERMS, defining the format of the reports and messages to be issued by the ERMS, providing dating and proof of transactions,...; they are employees of organisations managing an ERMS, such as publishers/producers, distributors, collecting societies, or they are employees of a TTP organisation that operates an ERMS on behalf of one or several publishers/producers, distributors and/or collecting societies.

Use rights administrators or URA

In some cases, the use right managers have to delegate some parts of their responsibilities to one or several use right administrators, who are located in the distributors and/or the collective end-user organisations: e.g. a CD-ROM acquired by an industrial firm will be installed by a local system manager, playing the role of a URA, who will record the authorised individual end-users, and have an ERMS monitor their utilisation of the CD-ROM, produce a detailed internal usage report for its management, and possibly produce a more synthetic external usage report for the publisher of the CD-ROM.

TTPs (Trusted Third Parties)

They are independent entities (persons, organisations, machines) which perform operations trusted and agreed by other parties such as end-users and service providers. TTPs could have roles such as: identification of agents and copyrighted applications, authentication of digital signatures, management of public keys, monitoring of usage operations, notarisation of proofs (usage reports). These roles could be played by neutral organisations, certifying the quality and confidence of URMs and ERMS attached to publishers/producers, distributors and collecting societies, or even operating ERMS on behalf of publishers/producers, distributors and/or collecting societies.

II. INTELLECTUAL PROPERTY LAW

1. Introduction

It is useful to recall that an ERMS is based on contractually defined clauses or terms that bind the various actors (authors, editors, producers, distributors, users,....). These contractual terms reflect the idea that all parties are free to decide on the terms of their contract with the important limitation however that the contract may not override mandatory legal provisions contained in an applicable piece of legislation. When designing an ERMS the first step is therefore to identify the correct copyright application and the corresponding applicable legal framework so as to draft contracts that are not contrary to the binding provisions contained in the legislation. The difficulty remains in practice, that copyright and neighbouring rights (including the sui generis right) exists without any formality of registration or deposit. There is no *a priori contro*l of originality or of substantial investment[6]. Any person can therefore consider that a work is protected by an IPR and include it in a ERMS.

•Once the protected work has been identified, the ERMS should be able to respect the *limitations* to the exclusive rights of the author, for want of a clear recognition of the binding nature of exceptions. Such limitations are contained in national copyright legislation and consequently vary from country to country[7]. Private copying, library and archival copying, educational exception, and quotation are examples of such exceptions to the exclusive rights of the author.

6 Concerning the data base protection

7 Dr P. Bernt Hugenholtz. *Copyright Problems of Electronic Document Delivery*. EUR. 16056 EN

2. Subject Matters of Copyright*

2.1. Introduction:

When creating and publishing a copyrighted application to be protected by an ERMS, a number of objects resulting from the creation could be protected by an intellectual property right, which raises the problem of obtaining clearance from rightholders. These intellectual property rights are also the rights to be managed by the ERMS in the Cited Model and could either be a copyright, a neighbouring right, a design right or a sui generis right.

In order to reproduce or include a work protected by an intellectual property right in a multimedia product, an authorisation has to be obtained from the right holder.

Since no deposit is required to enjoy copyright in creations, it is sometimes difficult to determine the correct copyright work and who the rightholder entitled to authorise the utilisation of the protected work is.

Therefore, the purpose of this title is to provide an overview of the various protections existing in European countries and in the United States so as to clarify the current copyright and related rights framework when seeking the necessary clearance.

The relevant rights to be addressed in this title are the copyright, the neighbouring rights, the sui generis right , the design right and the right on image. Such rights vest upon their rightholders the right to authorize the utilisation of the protected matter.

For each system of protection, the questions to be considered are what is protected, to what extent, how long and who owns the right.

2.2. Subject matters of copyright

Remark : The main differences between legal frameworks in European Member States and the United States as regards the protected works, the standard of originality, the duration of the right and the ownership, are illustrated in the table 1 (after point 1.4.2.).

---

* Author : Séverine DUSOLLIER

a. Protected Works

The Berne Convention states that the copyright protects any literary or artistic work. All national copyright Acts convey this principle albeit being subject to some minor differences from a country to another.

In most national regulations, the copyrightable subject matter needs to be original and expressed in a certain form.

Some legislations provide a non exhaustive list of protected works, which can help identify the objects that could be liable to copyright protection. These lists are more often not exhaustive, so that the mere fact that a work resists characterisation in terms of their established categories does not justify the non protection of this work.

For instance the list of the Berne Convention mentions the following copyrightable items:

"books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatico-musical works; choreographic works and entertainments in dumb show; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science[8]*."*

b. Standard of protection

Europe

The overwhelming opinion in European countries, with the exception of the United Kingdom to some extent, is that the works protected must be original. To be considered original, a work must display some expression of personality, however minimal, regardless of the kind, form of expression, merit or purpose of such work[9]. Case law has construed this

---

8 Berne Convention. Art. 2§1.

9 STROWEL. "Droit d'auteur et Copyright". Bruylant. Bruxelles. 1993. p. 468

requirement very broadly. For instance, furniture, silverware, jewellery, clothing, etc., might be copyrighted if they are original. In Germany, the standard of originality, which is defined as a personal intellectual creation, covers what is called the 'small change' of copyright, which includes catalogues, printed forms, cook books, address books, directories and so on[10].

A number of Copyright Laws also protect scientific works by copyright[11]. In this case, what is protected is not the scientific content of the work, but rather their (normally literary) form of expression.

Another particularity can be found in the Dutch legal framework which regards as protected works 'all other writings`, thus even that which are not original[12]. These non-original writings include telephone directories, broadcast programs listings, etc. The application of copyright rules to this 'pseudo-copyright' matter has to be decided for each provision separately according to its purpose. The protection granted by the courts has only been extended so as to prevent the copying of the writings themselves. However, this minimal protection should be sufficient to prohibit the unauthorised use of such writings on-line.

United Kingdom

The Copyright, Designs and Patents Act 1988 gives protection to a wide variety of works dissociated in two sub-headings[13]. The first one includes the original literary, dramatic, musical and artistic works (which used to be described as 'Part I Works') which are original works of authorship.

The requirement of originality means that the product must originate from the author in the sense that it is the result of a substantial degree of skill, industry or experience employed by him[14].

The second species of works, so called in the Copyright Act 'Part II: Subject Matters of

---

10 ibid., p. 438; NIMMER "International Copyright Law, p. FRG 18

11 This protection is explicitly provided by the German and Dutch Law

12 Art. 10(1) (1), Copyright Act; NIMMER, op. Cit., Neth-9; GROSHEIDE, Dutch Report, "Protection of authors and performers through contracts", ALAI Congress 1997, Montebello,

13 STROWEL, op. cit. , p. 466

14 University of London Press v University Tutorial Press [1916] 2 Ch. 601, "CORNISH "Material on Intellectual Property", Oxford, 1990, p.213

Copyright', are works covered by the Copyright Act of 1988 without being subject to the requirement of originality[15]. The purpose of their inclusion in the British copyright legislation is generally to protect the investment of the entrepreneur who embodies an author's work in a form in which it can be commercially exploited. Those are the following:

- Sound recordings
- Films
- Broadcasts
- Cable programs
- Typographical arrangement of published editions
- Computer generated works

These copyrightable objects meet specific rules as regards as the authorship of the right and the term of their protection[16].

United States

The American Copyright Act is designed to protect original works of authorship fixed in any tangible medium of expression. The words 'works of authorship' does not imply a standard of literary or artistic merit, for example, protection has been extended to telephone directories and personal letters.

The standard of originality does not include requirements of novelty. A work is original in American copyright law if it has not been copied from another source. To be a distinguishable variation of another work is sufficient to be liable to copyright. Therefore, a copy of something in the public domain will benefit from copyright protection if it is a 'distinguishable variation' of this work[17].

In the recent Feist decision[18], the Supreme Court has stated that the former doctrine of sweat of brow -which conveys the requirement of labour- is no longer sufficient, but that the work must display a minimum of creativity, which is closer to the European standard of originality.

---

15 J. PHILLIPS &A. FIRTH, "Introduction to Intellectual Property Law", Butterworths, London, 1990, chapter 12.

16 See fig. 1.

17 STROWEL, op. cit., p. 441

18 Feist, 27th March 1991, 799F. 2d 1219, 1226

Standard of protection defined in European Directives

The standard of protection is not harmonised at the European level. However, recent directives seeking to define the requirements of copyright in specific works, have adopted the same definition of originality. For instance, the Directive harmonizing the term of protection of copyright and certain related rights provides that the photographs are original in the sense that *they are the author's own intellectual creation*[19]. The Directives on the legal protection of computer programs and on the legal protection of databases use the same expression to define the standard of originality[20].

This standard, defined as the author's own intellectual creation, might become the guiding line of the forthcoming European definition of originality[21]. It must nevertheless be pointed out that national disparities will remain when providing an interpretation of what is to be considered as the author's own intellectual creation.

c. Term of the right

European Union

Regarding the duration of the right, the European Union has made a real effort of harmonisation by virtue of its directive 93/98/CEE of 29th October 1993. Consequently, the duration of the copyright is, in all European Member States, of 70 years after the death of the author[22].

The country of origin of the work is important in determining duration. Basically, if the country of origin is a European Economic Area (EEA) State, the provisions on duration set out in the Directive shall apply. If the country of origin is a non-EEA State, then the duration will be that provided for by the country of origin as long as this is no longer than the term provided in the directive. For example, works subject to US copyright will only enjoy a term of 50 years after the death of the author.

---

19 Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights. O.J. L290. 24/11/93. p. 9

20 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of software.. O.J. L 122. 17/3/91. p. 42: Council Directive 96/9/EEC of 11 March 1996. O.J. L 77/20. 27/3/96.

21 VIVANT. "L'incidence de l'harmonisation communautaire en matière de droits d'auteur sur le multimédia". Eur. Comm. . 1995. EUR 16068. p. 10

22 VIVANT, op. cit.. p. 94

The directive also prescribes the following particular rules:

"Art.1, §2: In the case of a work of joint authorship the term referred to in paragraph 1 (i. e. 70 years after the death of the author) shall be calculated from the death of the last surviving author.

Art. 1, §3: In the case of anonymous or pseudonymous works, the term of protection shall run for seventy years after the work is lawfully made available to the public. However, when the pseudonym adopted by the author leaves no doubt as to his identity, or if the author discloses his identity during the period referred to in the first sentence, the term of protection applicable shall be laid down in paragraph 1 (i.e. 70 years after the death of the author).

Art.1, §4: Where a Member State provides for particular provisions on copyright in respect of collective works or for a legal person to be designated as the rightholder, the term of protection shall be calculated according to the provisions of paragraph 3 (i.e. 70 years after the work is lawfully made available to the public), except if the natural persons who have created the work are identified as such in the versions of the work which are made available to the public. This paragraph is without prejudice to the rights of identified authors whose identifiable contributions are included in such works, to which contributions paragraph 1 and 2 shall apply.

Art.1, §5: Where a work is published in volumes, parts, instalments, issues or episodes and the term of protection runs from the time when the work was lawfully made available to the public, the term of protection shall run for each such item separately.

Art. 1, §6: In the case of works for which the term of protection is not calculated from the death of the author or authors and which have not been lawfully made available to the public within seventy years from their creation, the protection shall terminate.

Art. 4: Protection of previously unpublished works

Any person who, after the expiry of copyright protection, for the first time lawfully publishes or lawfully communicates to the public a previously unpublished work, shall benefit from a protection equivalent to the economic rights of the author. The term of protection of such rights shall be 25 years from the time when the work was first lawfully published or lawfully communicated to the public.

Art. 5: Critical and scientific publications.

Member States may protect critical and scientific publications of works which have come into the public domain. The maximum term of protection of such rights shall be 30 years from the time when the publication was first lawfully published.

Art. 8: Calculation of terms

The terms laid down in this Directive are calculated from the first day of January of the year following the event which gives rise to them."

In the case of audio-visual works the Directive prescribes that the principal director thereof shall be regarded as the author of the work, while stating a particular rule for the term of protection:

Art. 2, §2: The term of protection of cinematographic or audio-visual works shall expire 70 years after the death of the last of the following persons to survive, whether or not these person are designated as co-authors: the principal director, the author of the screenplay, the author of the dialogue and the composer of music specifically created for use in the cinematographic or audio-visual work.

This particular provision can lead to a puzzling situation as in the United Kingdom where the authors of a audio-visual work are completely different from the persons whose death is the reference for the copyright duration[23].

United States

The term of the copyright in the United States is of 50 years after the death of the author[24].

Regarding the joint works, the term is calculated since the death of the last surviving co-author, as in Europe.

In the case of an anonymous work, a pseudonymous work or a work made for hire, the copyright endures for a term of 75 years from the year of its first publication , or a term of 100 years from the year of its creation, whichever expires first. (if the author of an anonymous or a pseudonymous work make known his identity in the records of a registration, the general term will apply).

After a period of 75 years after the first publication of a work, or a period of 100 years of its creation, whichever expires first, any person who obtains from the Copyright Office a certified report that the records disclosed nothing to indicate that the author of the work is

---

23 D. BAINBRIDGE, "Changes to the duration of copyright", CLSR 1996, n°12, p. 238 ; CORNISH, "Recent changes in British copyright Law", RIDA, n°172, April 1997, p. 173

24 USC- Copyright - Title 17- § 302

living, or died less than fifty years before, is entitled to the benefits of a presumption that the author has been dead for at least fifty years[25].

The general rules, as described above, apply only to works created on or after the 1st January 1978. Since specific rules of deposit and registration applied before this date, the duration of copyright in the works created beforehand is subject to particular and complicated provisions[26].

d. Ownership of the right

Principle

As a general rule, the author of the work will be the natural person who actually creates the work: the writer of the text, the composer of the music.

In cases where the author can not be identified, this principle is subject to some adaptations so as to consider an identified person as the author, vis-à-vis third parties at least.

For instance, the publisher of an anonymous or pseudonymous work is deemed, vis-à-vis third parties, to be its author. As soon as the author makes himself known, he resumes the exercise of his right. In most legal systems, any person under whose identity (whether his name or a mark enabling identifying him) the work is disclosed is deemed to be the author [27]. These presumptions can be subject to the proof of the contrary.

Regarding posthumous works, some legislations provide that copyright is granted to the owners of the material embodiment of the posthumous work, although these owners are not necessarily the author's heirs.

---

25 For example, an author writes and publishes a book in 1978. He died in 2020. There is no record of his death in the Copyright Office. As a principle, the copyright in his work will endure until 2070.

In 2058 (so after 75 years from the first publication of the work), an editor wants reproduce the book. He obtains from the Copyright Office the report as referred above. The author is consequently presumed being death at least in 2008. The editor is therefore entitled to reproduce the work which is presumed be fallen in the public domain.

26 See USC- Copyright - Title 17- § 303 & 304.

27 Berne Convention, art. 15.

Joint works

Two types of joint works need to be distinguished. Firstly, joint works might be the outcome of co-operation between authors such that the contribution of each author can no longer be separated from the whole work, with the result that contribution can not be a separate object of artistic evaluation outside the context of the whole work.

For these works, most regulations provide that the exercise of the right should be determined by an agreement between all co-authors. In the absence of a prior agreement, any act of exploitation of the work requires the consent of all of its co-authors. In case of conflict, any co-author can petition the court to resolve the matter.

Contrary to this principle, the Dutch Law provides that copyright in joint works may be enforced by any of the co-authors, unless otherwise agreed.

Secondly, another type of joint works are works where each contribution can be separated from the others and be the object of a distinct exploitation, such as films, operas, etc. In this case, each author can exercise individually his rights, provided that such separate exploitation does not prejudice the exploitation of the common work.

Besides, collective works are defined in some countries, such as France, as *works created by the initiative of the natural person or legal entity who edits it, publishes it and discloses it under his direction and name, and in which the personal contributions of the various authors participating in its development are merged in a totality arising out of its original conception, so that it is impossible to attribute to each of said authors a separate right in the total work thus produced"*[28]. In this case, the copyright vests upon the person who edits and discloses the collective work under his direction and name.

---

28 French Law on Intellectual Property. Ist july 1992. Art. L. 113-2

Figure 1 : General rules of copyright

Country	Subject Matters	Requirements		Duration	Ownership
		Fixation	Originality		
BELGIUM	Literary and artistic works	YES	the work must display some expression of personality	70 years after the death of the author	Natural person *Presumption : person under whose name the work is disclosed*
FRANCE	Literary and artistic works	NO	the work must display an original or personal character	70 years after the death of the author	Natural person *Presumption : person under whose name the work is disclosed*
GERMANY	Literary, scientific and artistic work	NO	personal intellectual creation	70 years after the death of the author	Natural person *Presumption : person who is designated in the customary manner as the author of the original of the work or on copies thereof; by default of such a mention, the editor is presumed to be entitled to exercise the author's rights.*
NETHERLANDS	Works of literature, art or science Non-original writings	NO NO	works which, as the result of creative labour, show a original or personal character NO	70 years after the death of the author	Natural Person *Presumption : Whoever is indicated as the author in or on the work or whoever is made known as the author by the party making the work public.*
UNITED KINGDOM	I. WORKS: original literary, dramatic, musical or artistic works	YES	the work must result from a substantial degree of skill, industry or experience	70 years after the death of the author	Author

	II. COPYRIGHT :	YES	NO	50 years from the first commercial exploitation	
	1. Sound recordings	YES	NO	50 years from making or from release, if published or disseminated	1. Person by whom the arrangements necessary for its making are undertaken
	2. Cinemato-graphic films	YES	NO	70 years from the death of the last survivor of : the director, the author of the screenplay, the author of the dialogue, the composer of the music	2. Person by whom the arrangements necessary for its making are undertaken = Producer/director
	3. Cable programs	NO	YES	50 years from release	3. Person who provide the cable programme service
	4. Published edition of a work	YES	NO	25 years from the first publication	4. Editor
	5. Sound and TV Broadcasts	NO	NO	50 years from broadcasting	5. Broadcasting company
	6. Computer generated works	NO	NO	50 years from the creation	6. Person who makes the arrangements necessary
UNITED STATES	Intellectual works	YES in any tangible medium	Independent Creation	50 years after the death of the author	Author (Natural person or legal entity) *Presumption : Person or entity mentioned as the author in the certificate of registration issued by the Copyright Office where the work is registered*

Specific case of audio-visual works

The ownership of audio-visual works used to be one of the most controversial issues in international copyright law[29].

Two European Directives[30] recently settled the controversy by prescribing that the principal director of a cinematographic or audio-visual work shall be regarded as its author or one of its authors. Member States may nevertheless provide for others to be considered as its co-authors[31].

As a consequence, some disparities between Member States still subsist in the definition of the co-author of a audio-visual work[32]. A number of Member States also provide presumptions of assignment of exploitation rights to the producer. unless otherwise agreed. In most cases, this presumption can only be construed in the sense that nothing but the rights useful for the exploitation of the audio-visual work are presupposed to have been waived. The question whether the scope of exploitation covers the digitization and on-line transmission is still unresolved in most countries.

The figure hereafter provides for an overview of the legal rules in different countries:

---

29 " Audio-visual Works and literary and artistic property". proceedings of ALAI Congress. Paris. Unesco, 17-22 September 1995.

30 Council Directive harmonizing the term of protection of copyright, op.cit., art. 2,§1. Council Directive 92/100 of 27 Novemher 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property. of L346/61, art. 2,§2

31 REINBOTHE & VON LEWINSKI, "The EC directive on Rental and Lending rights and on piracy", Sweet & Maxwell, London, 1993, p. 47

32 K. JORNA, M. MARTIN-PRATT, "New rules in European Copyright", EIPR 1994, n° 4, p. 147

Figure 2 : Authorship of audio-visual works

COUNTRY	AUTHORSHIP	PRESUMPTION
Belgium	Principal author : - director The following are presupposed to be co-author (subject to the proof of contrary) : -author of the screenplay - author of the dialogue - author of the adaptation - author of musical composition specially composed for the audio-visual work -graphic author for works of animation which represents an important part of the audio-visual work - authors of the pre-existing work if their contribution is used in the new work	The right of exploitation is presupposed to have been waived to the producer. except for rights in musical works
France	-director -author of the screenplay - author of the dialogue - author of the adaptation - author of musical composition specially composed for the audio-visual work - authors of the pre-existing work if their contribution is used in the new work	The right of exploitation is presupposed to have been waived to the producer. except for rights in musical works
Germany	-director -cameraman - editor (some legal commentators mention other co-authors)	The right of exploitation is presupposed to have been waived to the producer
United Kingdom	For films made before 1st July 1994 : -Producer For films made after 1st July 1994 : -Director -Producer	No presumption since the producer is co-author

Netherlands	There is not a list in the copyright act. but the commentators mention : - director - author of the screenplay - executive producer - director of photography - choreographers - editor - cartoonist - music composer	The right of exploitation is presupposed to have been waived to the producer. except for rights in musical works
United States	If the work .is made for hire (in most cases) - Producer Otherwise. joint work whose authors can be the writer. the director. the producer. the camera operator, the film editor and others.	No presumption since the producer is deemed to be the author

Works made for hire

A major exception to the principle of the natural creator of the work as the author, is the case where the works are created in the course of the employment or where the work has been commissioned by another person. In those cases authorship might be attributed, sometimes fictively, to persons and legal entities who may not be, in the natural sense of the word, the "author". For instance, a number of countries, such as the Netherlands, the United Kingdom or the United States, provide that the employer or the commissioner shall be regarded as the author of the work, at least for the economic rights.

In this case, the employer or commissioner is treated as the owner of the right but is not deemed to be the author which implies, for example, that the duration of copyright is still measured by reference to the life of the actual author. On the other hand, in the United States, the employer is the author at the outset and a specific term of the right, without any reference to the actual creator, is prescribed by the law[33].

33 See supra.

Figure 3 : Authorship of works made for hire :

Country	Distinction	Ownership
Belgium	Employment	Creator of the work (unless otherwise agreed), except: -software : employer
	Commissioned works	Creator of the work (unless otherwise agreed)
France	Employment	Creator of the work (unless otherwise agreed), except: - software : employer - journalists : owner of the newspaper or periodical in so far as the copyright relates to periodical publication
	Commissioned works	Creator of the work (unless otherwise agreed), except : - commissioned works in advertising : exploitation right in the work belongs to the commissioner
	Collective works	Person who edits and discloses the work under his name
Germany	Employment	Creator of the work (unless otherwise agreed), except for software : employer
	Commissioned works	Creator of the work (unless otherwise agreed)
Netherlands	Employment	Employer (economic and moral rights)
	Under the supervision of another person	The supervising person
	Corporate works	Person who makes the work public as its own
United Kingdom	Employment	Employer
United States	Employment	Employer
	Commissioned works	Commissioner, provided : - a written document says so, and - it is a contribution to a collective work as part of a audio-visual work, as translation, as a supplementary work, a instructional text, as a test, as an atlas.

Transfer of rights

In a number of cases, the initial owner has waived or assigned his economic rights to an editor or a producer, who will be the only person entitled to grant authorisation to use the work. The contract between the author and the editor or producer has to comply with particular rules whose purpose is to protect the author. These rules are generally that the contract must be written, that a transfer of still unknown ways of exploitation is void[34] and that the duration and the scope of the grant of rights must be expressly stated.

The obligation of providing the scope of the transfer implies that the rights which are not expressly, or implicitly for some countries, waived by the author remain with him.

In France and Belgium, each way of exploitation has to be written in the contract. In Germany, the scope of the transfer will be construed pursuant the 'purpose of grant', which can cover implicit assignments. In the Netherlands, the editor is only entitled to exercise the rights specifically mentioned in the instrument of transfer or the rights necessarily implied from the nature or purpose of the title evidenced by the deed[35].

In the United States, the interpretation of the scope of a grant are a matter of state laws, which can considerably vary[36]. However, the federal copyright law provides for recordation in the Copyright Office of transfers of copyright ownership, which can facilitate the identification of the actual rightholder.

In conclusion, even if the author has granted his economic rights to another person, the actual scope of this transfer may not cover the digitization or the on line exploitation, either because the digitization was unknown as entering the assignment contract or because the scope of the transfer is not sufficiently explicit.

2.3. Neighbouring Rights

---

34 For example, in France, Belgium and Germany. Consequently, any transfer of rights made before the technology of numerisation is known can not cover the digitisation of the work.

35 GROSHEIDE, Dutch Report, ALAI Congress 1997, p.3-4

36 WECHSLER, US National Report, ALAI Congress 1997, p. 5

a. Scope of the right

The European Directive on the lending and rental right has harmonised the rightholders of neighbouring rights[37], which are the following:

- the performers (actors, singers, musicians, dancers and other persons who act, sing, deliver, declaim, play in, interpret, or otherwise perform literary or artistic works);
- the producer of phonograms in respect of his phonograms;
- the producer of the first fixation of a film, in respect of the original and copies of their films;
- broadcasting organisations in respect of fixations of their broadcasts.

The Directive provide them with the following rights:

- For performers: the exclusive right to authorize or prohibit the fixation of their performance

- For broadcasting organisations: the exclusive right to authorize or prohibit the fixation of their broadcasts

- For all:

  - the reproduction right;
  - the right of broadcasting and communication to the public;
  - the distribution right;
  - the lending and rental right.

In the United States, no protection of performers' rights and other related rights is provided since the movie majors are strongly opposed to this. However, the recent WIPO Diplomatic Conference enacted a Treaty on performances and phonograms which endowed the performers and producers of phonograms of rights of reproduction, distribution, rental and communication. This does not cover the rights of performers in the audio-visual fixations of their performances.

---

37 VIVANT, op. Cit., p. 78

b. Duration[38]

The related rights shall expire 50 years

- after the date of performance, for performers
- after the date of fixation for producers of phonograms and for producers of first fixation of a film
- after the first transmission of a broadcast, for broadcasting organisations.

c. Presumption of transfer

In a number of countries, the copyright law provides for a presumption of transfer of the performers' rights to the film producer, such as in France, Germany, Belgium, the Netherlands. In the United Kingdom, no presumption of transfer of performers' right to the film producer is provided.

2.4. Protection of databases

Since a directive of 1996 , the databases are protected either by copyright, either by a sui generis right of 15 years, for lack of originality. Therefore, an authorisation of the rightholder is needed before reproducing and utilising a database. Since this protection is also particularly relevant for the operation of the ERMS as regards the copyrighted application, an in-depth analysis of the Directive is considered in the next title.

2.5. Protection of industrial designs

In certain projects, such as TISSUS, the protected information shall also consist in reproductions of industrial designs. Such reproductions and uses must be authorised by the

38 Art. 3 of the Council Directive on the term of protection of copyright and related rights.

creator of the design either by virtue of a copyright, if his creations are original, either by virtue of a specific protection, set out in the national design laws[39]. Both protections might be cumulative or exclusive. A project of a European Directive on the protection of Industrial Designs is still waiting to be adopted[40].

All systems, require that the design has to be registered or deposited to be protected, although, in some countries, a shorter protection is provided for unregistered designs[41]. Registration usually leads to publication of design. The standard of protection for a registrable design is novelty, albeit the definition of this requirement varies from a country to another.

This project of Directive defines the design as "the appearance of the whole or a part of a product resulting from the specific features of the lines, colours, contours, shape and/or materials of the product itself and/or its ornamentation".

The following figure will provide for an overview of the current legal framework in the main European countries, as well as the proposed protection of the project of Directive.

Country	**Standard of Protection**	**Maximum Duration**	**Protection by copyright**
Benelux	Novelty: not notorious in Benelux commercial design circles within the last 50 years or not anticipated by prior Benelux deposit	up to 3 periods of five years= 15 years	YES : requirement of "marked artistic character"
France	New or distinctive . Original when created	up to 2 periods of 25 years = 50 years	YES: widely available for designs which are not patentable. The French Intellectual Property Law protect by a copyright the 'fashion creations'

39 A. FIRTH, "Aspects of design Protection in Europe", E.I.P.R. 1993, n°2, p. 42-46.

40 Proposed Community Design Regulation and Directive. (94/C 2902) COM (93) 342 FINAL. (93/C 345/09) COM (93) 344 FINAL. submitted by the Commission on 3/12/93. O.J. 23/12/93, p.1 & O.J. 31/01/94, p.20.

41 For instance in UK and in the Proposal of Directive.

Germany	Known to German trade circles Original - personal intellectual creation	up to four periods of five years = 20 years	(High) artistic merit
United Kingdom	Novelty : local	up to five periods of five years = 25 years	YES : artistic work
Proposed Directive	Novelty : if no identical design has been made available to the public before. And individual character: if the overall impression it produces on the informed user differs significantly from that produced by previously existing designs	Unregistered design : 3 years from the date when they are made available to the public Registered Designs : up to five periods of 5 years = 25 years from the date of application for registration	

2.6. Right on image

A specific rule exists in the Belgian Copyright Law which provides *that "neither the author nor the owner of a portrait has the right to reproduce it or exhibit it publicly without the consent of the person depicted or else without that of his heirs or successors in interest during twenty years following his death*"[42].

This protection applies to all forms of portraits : paintings, sculpture, drawing, photography, film. The case law has admitted that the authorisation of a public person to reproduce his portrait shooting during his public life is presumed. A similar rule exists in France in the Criminal Code.

Under British law, those who commission photographs and films for private or domestic purposes are entitled to object to their public exposure[43].

---

42 Belgian Copyright Act. Art. 10

43 Copyright. Designs and Patents Act 1988. s.85

Conclusion

In the process of seeking the necessary clearance of rights when developing a multimedia product and protecting it by an ERMS, the following questions have to be considered :

- Is the object to be reproduced and included in the multimedia work protected by a intellectual property right ?
- Which intellectual property right is it ? Copyright, neighbouring rights, sui generis right, design right ?
- In the case of the copyright :
    - Is the work original ?
    - Is the duration of the right expired ?
    - Who is the rightholder (initial or by assignment of the right) entitled to authorize the use of the work ?
- In the case of neighbouring right :
    - Which neighbouring right is it ?
    - Is the duration of the right expired ?
    - Who is the rightholder entitled to authorize the use of the work ?
- In the case of databases :
    - Is the database original ? If yes, the questions concerning the copyright are to be addressed. If no, The following questions are to be addressed :
    - Who is the maker of the database ?
    - Is the duration of the right expired ?
- In the case of designs :
    - Is the design novel ?
    - What is the duration of the right ?

- Who is the rightholder of the design right ?
- Is the design protected by a copyright ?

Such questions constitute a necessary frame to identify the protected objects and the correct rightholders from whom an authorization to use the work is required.

Nevertheless, some major disparities still exist in the legal frameworks of Member States and of the United States which entails a proper consideration of any legislation where the final work will be disseminated.

3. Protection of Databases*

Introduction

On the 11th of March 1996, the 5th EC directive in the field of copyright and related rights was enacted. The "data base directive" has been predicted in the Commission's Green Paper on Copyright and Related Rights in the Information Society as having fundamental importance in the information society given the fact that most of the new products and services will be operated from data bases[44]. It is also recognised in the data base directive itself[45] that they will also be of used in many other fields.

It has become apparent over the past few months in the COPEARMS project that Vertical consortia wishing to use an ERMS are faced with the issue of determining the "copyright application" which can be a literary work, a photograph, an audio-visual work, a computer program,... or a data base. The purpose of this document is to provide an overview of the rules contained in the recently adopted data base directive.

1. Definition

Data bases are defined widely in article 1.2 as meaning a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. It is specified in the recitals of the directive that electronic data bases may also include devices such as CD ROM or CD I[46].

The directive provides for a two tier system of protection by copyright or by a new so called *sui generis* right.

---

* Author : Michèle LEDGER

44 Brussels, 19.07.1995, COM(95)382 final, p. 31.

45 Recital n°9.

46 Recital n° 22.

2. Protection by copyright [47]

Data bases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected by copyright[48]. Such protection only covers the structure of the data base and does not extend to the contents and the rights subsisting therein[49].

The author of the data base[50] has the exclusive right to authorise

(a) temporary or permanent reproduction by any means and in any form, in whole or part;

(b) translation, adaptation, arrangement and any other alteration;

(c) any form of distribution to the public;

(d) any communication, display or performance to the public;

(e) any reproduction, distribution, communication to the public of the acts referred to in (b)[51].

As all prior directives in the field of copyright, moral rights are outside the scope of the directive. Moral rights nevertheless belong to the author and should be exercised according to legislation of the Member States and the provisions of the Bern Convention for the protection of Literary and Artistic Works[52].

The last article in chapter 2 deals with the exceptions to the restricted acts. The lawful user of a data base is allowed to perform any of the restricted acts listed above, without the authorisation of the author of the data base whenever they are necessary for the purposes of access to the contents of the data base and normal use of the contents. Any contractual provision contrary to this rule shall be null and void[53]. Furthermore, when implementing the

---

47 Chapter 2 of the directive.

48 Article 3.1..

49 Article 3.

50 That is to say the natural person or group of natural persons who created the data base, or where the legislation of the Member State so permits, the legal person designated as the right holder by that legislation (article 4.1.). It is also specified in the whereas clauses that arrangements applicable to data bases created by employees are left to the discretion of the Member States.

51 Article 5.

52 Recital n° 28.

53 Article 15.

directive into national legislation, member States shall have the option of providing for limitations on the rights in certain cases which are limitatively listed in article 6. 2.including :

(a) in the case of reproduction for private purposes of a non-electronic data base[54];

(b) Where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved.

3. *Protection by the* sui generis *right*

The most innovative feature of the directive is the creation of a new form of protection which is called the sui generis right. The directive also aims at protecting the makers of the data base against misappropriation of the result of the financial and professional investment made by protecting the whole or substantial part of the data base. The substantial part of the data base may be evaluated quantitatively and/or qualitatively.

The rule is that the maker of a data base which is made available to the public may not prevent a lawful user from extracting and/or re-utilising insubstantial parts of its contents[55]. Nevertheless, lawful users may not perform acts which conflict with the normal exploitation of the data base or unreasonably prejudice the legitimate interests of the maker of the data base and may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the data base[56] since as it is recalled in the directive, protection of data bases under the sui generis right applies without prejudice to the rights existing in their contents[57]. Any contractual provision contrary shall be null and void[58]. As in chapter II on copyright protection, optional exceptions[59] to the sui generis right are provided in the directive. Member States, when implementing the directive into national legislation may provide for example that lawful users of a data base, which is made available to the public may, without, of its maker extract or re-utilise a substantial part in the case of extraction for private purposes of the contents of a non-electronic data base.

---

54 It is worthwhile noticing that while Member States are allowed to grant users a right of reproduction for private purposes in relation to non-electronic data bases. this option is not provided in so far as electronic data bases are concerned.

55 Article 8.1..

56 Article 8. 2 and 3.

57 Article 7. 4..

58 Article 15.

59 Article 9.

The sui generis right lasts for 15 years from the date of completion of the making of the data base or from any substantial change to the contents of the data base, evaluated qualitatively or quantitatively, so long as this results in the data base being considered to be a substantial new investment[60].

4. Entry into force

Member States were obliged to bring into force their laws, regulations and administrative provisions necessary to comply with this directive before 1 January 1998. Nevertheless, a number of Member States are late.

60 Article 10.

4. RIGHTS OF EXPLOITATION AND EXCEPTIONS*

The Copyright Act gives the authors exclusive rights with respect to the use of their work (article 17 and following).

The consequence, in an on-line delivering of copyrighted material environment, is that a previous consent will be necessary from the rightholder.

This is particularly the case for all reproductions (copies) of the work, all communications to the public as well as all adaptations and translations.

The purpose of this title is provide an overall overview of the exclusive rights of the author and other rightholders. Such rights will be entitled to be managed by the ERMS.

4.1. Rights of exploitation

a. Economical rights

i) Right of Reproduction (article 18)

This right grants the author the right to authorize or prevent the reproduction of the work in any form.

The act of reproduction includes acts such as the digitisation of a work, or acts such as uploading or dowloading of a work to or from the memory of a computer.

Actually, the on-line transmission of works or prestations protected by an intellectual property right implies a number of transient and technical electronic reproductions of works.

Whether such reproductions are covered by the scope of the reproduction right as defined in most Member States, is still uncertain, which justify the necessity to provide for a harmonised definition of this right of reproduction.

---

* Author : Jean-Christophe LARDINOIS

In the Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society[61], the definition finally adopted is :

" *the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part.* "

The same definition was submitted to the WIPO Diplomatic Conference by the European Commission, but was finally not adopted , due to a strong opposition to the inclusion of the temporary reproduction in the restricted acts.

Such a definition conveys clearly that temporary and transient reproduction is subject to the exclusive right of the rightholder.

Nevertheless, an exception to this reproduction right with regards to this particular technical reproduction is put forward in the article 5 (1) of the proposal, which states that "temporary acts of reproduction which are an integral part of a technological process for the sole purpose of enabling use to be made of a work or other subject matter, and having no independent economic significance, shall be exempted form the right set out in Article 2".

This provision seeks to take into account the concerns of service and access providers concerning the incidental acts of reproduction. "Browsing" or "caching" may thus not be restricted acts if it comply with particular requirements set out in art. 5(1)[62]. The transposition of this exception of temporary acts of reproduction will be obligatory for the Member States.

Another important element of the definition refers to the direct and indirect reproduction. The term "direct" means reproducing a work or other protected subject matter directly onto the same or a different medium.

The term "indirect" covers reproduction done via an intermediate stage, for example, the recording of a broadcast which itself has been made on the basis of a Phonogram[63].

The right of reproduction is enjoyed by copyright and neighbouring rights holders.

---

61 10.12.1997 COM (97) 628 final. Hereinafter. the Proposal

62 Recital 23 of the Directive

"Copyright and Related Rights in the Information Society - Proposal for Directive/Background", http://europa.eu.int/comm/dg15/en/intpropo/intprop/1100.html. p.7

63 Explanatory Memorandum. Comment on article 2. point 3.

ii) The right of communication to the public (article 20)

Through this right, the rightholder controls the direct communication to the public (without any tangible objets) of works.

This right has been recently defined by the WIPO organisation and the Proposal (article 3) as the right to communicate works to the public, including the right of making available works in such a way that members of the public may access them from a place and at a time individually chosen by them. Consequently, this right covers the on-demand acts of exploitation of works.

The neighbouring rights holders enjoy only from an exclusive right for making available which is thus limited to on-demand transmissions. For other communications, they enjoy from a simple right of remuneration.

iii) Right of adaptation / translation

The rightholder benefits from the right to authorize the translation, the adaptation or any transformation of works.

The right of adaptation consists mainly of the transposition of the work in a different type indeed a different medium.

iv) Right of distribution

Article 4(1) of the Proposal provides for authors the exclusive right of authorising any form of distribution to the public, by sale or otherwise, of the original and copies of their works.

Both new treaties (WCT and WPPT) contain also an exclusive right of distribution, namely the right to authorise or prohibit the distribution of fixed copies as tangible objects (e.g. on paper, CD, CD ROM, tape, as opposed to on-line form). The distribution right does thus not apply to services in general or on-line.

The second provision sets out that the distribution right is only exhausted in the whole of the Community upon the first sale of the copy of a work in the Community, providing that the sale is made by the rightholder or with his consent. Under this principle, once an author has agreed that tangible copies of his work may be sold in one Member State, these copies can be sold throughout the EU without requiring a new authorisation from the rightholder.

This latter provision meets finally the view of the Diplomatic Conference which decided that it shall be a matter for Member States to determine the existence and the conditions of the exhaustion of the distribution right[64]. Consequently, the Proposal has chosen the principle of community exhaustion while providing that the distribution right should not be exhausted after a first sale outside the European Union[65].

b. Moral Rights

Beside the economical rights, the authors benefit also from moral rights (article 14 Copyright Act) which constitute the expression of the existing link between them and their creation.

These rights consist of three main prerogatives :

- the *right to disclose* the work which is the right for the author to decide when his work is finished and how, when, and under which circumstances it should be made accessible.

- the *right of attribution of authorship* which is the right for the author to have authorship of his works attributed to himself, to prevent others from attributing authorship of his works falsely to themselves or others, and to refuse to have his authorship of a work recognized.

- the *right of integrity* which entitles the author to relief against any material or intellectual alteration or impairment to his work

This last prerogative is the most important in a digital environment which involves alterations even light and partial of the work before beeing retransmitted sometimes by the author, sometimes by other users.

It is worth to mention that moral rights are in some countries (e.g. France) "inalienable".

---

64 WCT, art. 6 (2).

65 Recital 18 of the Proposal

4.2. Exceptions

a. National level

The exclusive rights of the author are not absolute and suffer in some cases some exceptions which allow either a free use of the work (exception to the exclusive rights) or an use without the author's consent.

The exceptions systems vary largely from a country to another. Therefore, we will focus on the exceptions provided in the recent Proposal for an European Directive on Copyright in the Information Society which seeks to harmonise the exceptions.

b. EC level

The Proposal seeks to introduce an harmonization of the limitations and exceptions to the reproduction right and the communication to the public right.

The list set out in this provision is exhaustive what entails that national legal systems would not be allowed to maintain any exceptions to copyright other than those enumerated.

But, apart from the exception for temporary reproduction mentioned above, the implementation of these exceptions is only facultative.

Thereby, it shall be a matter for each Member State to decide which exceptions he will transpose in its legislation.

The harmonisation foreseen by the proposal is thus relative, since after the transposition of the directive in national laws, the systems of limitations to copyright could still comprise a number of disparities from a country to another both in the actual exceptions in force as in their scope and interpretation.

It is worthwhile to mention that it is still a Proposal which is strongly discussed at present in the European Parliament. In all likelihood, the list of exceptions will be subject to many changes even if minor.

i) Exceptions to the reproduction right

Article 5(2) (a), (b) and (c) sets out three optional exceptions to the reproduction right :

- Article 5(2) (a) allows Member States to maintain or introduce an exception for photo/print type reproduction ("reprography"), with or without a remuneration scheme.

Such reprography is limited to techniques of reproduction allowing a paper print. So the result of the reproduction must be in paper form.

- Article 5(2) (b) allows for exceptions reproduction of audio and audio-visual material for private use and for non-commercial ends

This provision does not make any distinction between analogue and digital technology. With regards to the digital private copying, the Commission has considered it premature at this stage to provide for a more harmonised solution, since it is still largely unknown whether such copying will be a widespread activity of consumers or not[66]. Therefore, a consultation of interested parties will take place by the end of 1998 so as to envisage further action in this field.

- Article 5(2) (c) allows Member States to exempt certain acts of reproduction from the reproduction right to the benefit of establishments which are accessible to the public, which are not for direct or indirect economic or commercial advantage, such as public libraries and archives

This exception does not apply to the communication to the public right.

Thus, the making available of a work by a library from a server to users on-line should and would require a licence of the rightholder or his intermediary and would not fall within a permitted exception

It is stated in the Explanatory Memorandum that the communication of copyright protected material via the homepage or website of a library will in many cases be in competition with commercial on-line deliveries of material since perfect quality copies of any work could be made available to a large number of users, whether on-site (with a multiplicity of screens in the library) or off-site (to other libraries or

66 Explanatory Memorandum of the Proposal. Comments on article 5.

remote users)[67].

This lack of exemption for libraries could be one of the key question in the progress of the adoption of this directive.

In our view, we regret that no distinction has been made between the on-line transmission of protected works by a library and the possibility for a library to make available works within the physical site of the establishment in specific and justified cases. In this latter case, a remuneration scheme could have been put forward.

ii) Exceptions to the communication to the public right and to the reproduction right

Article 5(3) provides Member State with the possibility of certain limitations to article 2 (the reproduction right) and article 3 (the communication to the public right).

Article 5(3) (a) allows Member States to exempt the use of a work or other subject matter (such as a sound or visual recording) or parts of it, provided that such use exclusively serves the purpose of illustration for teaching or scientific research, as long as the source is indicated.

In any case, only the part of the use which is justified by its non-commercial purpose may be exempted from the exclusive right.

Paragraph 3(b) to (e) allow Member States to provide for further exemptions to the reproduction right and to the communication to the public right, so as follows :

- for uses to the benefit of visually-impaired or hearing-impaired persons, which are directly related to the disability and of a non-commercial nature and to the extent required by the specific disability (handicapped persons);

- use of excerpts in connection with the reporting of current events, as long as the source is indicated, and to the extent justified by the information purpose (news reporting);

- quotations for purposes such as criticism or review, provided that they relate to a work or other subject matter which has already been lawfully made available to the public, the source is indicated, their making is in accordance

67 Directive Background, op. Cit., p. 9

with fair practice and to the extent required by the specific purpose (quotations);

- use for the purposes of public security or for the purpose of the proper performance of an administrative or judicial procedure (public security uses and uses in administrative and judicial proceedings).

iii). Scope of the exceptions.

As stressed in Article 5(4), limitations and exceptions have to be confined to certain specific cases and may not be interpreted in such a way as to their application to be used in a manner which unreasonably prejudices the rightholders' legitimate interests, or conflicts with normal exploitation of the protected subject matter.

It is the so-called 'three step test' enshrined in the art. 9(2) of the Berne Convention and confirmed in the recent WCT and WPPT.

5. The nature of copyright exceptions*

5.1. The balance of rights facing the Information Society

In a digital world wrapped by technological devices, the user won't be able to exercise the exemptions to copyright in the same way than in the physical world. In this last case, the copyright exemption was primarily used as a defence in litigation for copyright infringement. The user who had made an unauthorised reproduction or communication to the public of a protected work is allowed to argue that such an act was covered by a copyright exemption. Whatever his success will be, the user can enjoy from the exemptions system in a reasonable extent. A proper balance between the interests of the copyright holder and that of users or that of the society as a whole is maintained. In the digital world, the function of exemptions system will be completely different. If any act of reproduction or communication of a copyrighted work is inhibited by a technological protection, the user will have either to sue the rightholder for enabling him to exercise his exemption (for instance for research, education, criticism purpose); either to deploy some skill for circumventing the technical measure. In both cases, the burden imposed on the user is rather heavy. The exemption will resume its function of defence only in the case of an action brought against the user for having circumvented the system. This is why we can reasonably fear, as some commentators[68], that the balance embedded in most copyright regimes is threatened.

All these exceptions necessarily imply carrying out a rectricted act, whether it is an act of reproduction or an act of communication. Such act is precisely that inhibited or prevented by the technological measure.

Nevertheless, it is worth mentioning that the technological protection are not necessarily aimed at preventing access to public domain or exercise of exceptions. For instance, a system such as ERMS could be useful to monitor the access to administrative documents or the right of remuneration for private copy. But, in any case, the nature of exceptions should be considered, namely to provide for some legal certainty in that respect.

A lot of legal commentators argue for a recognition of the binding nature of the copyright exemptions. The consequence thereof would be that neither a contract nor a technology could

---

* Author : Séverine DUSOLLIER & Michele LEDGER

68 SAMUELSON, The Copyright Grab, Wired 4.01

GUIBAULT, Contracts and Copyright Exemptions, Institute For Information Law, 1997;

HUGENHOLTZ, Keynote Speech, Limitations and exceptions to copyright, Imprimatur Forum, october 1997, Amsterdam.

override the exemptions. There is very little literature or case law about the binding nature of all or some of these exceptions. Let us just cite to be provocative Th. HOEREN when he says that "The exemptions may not be restricted by contract. It is not possible to forbid private copying in the case of statutory licence." This position would be supported in the UK and Ireland on the basis that copyright is a limited monopoly right granted by statute. The copyright owner would not have the power to restrict a statutory license since his monopoly was granted on the basis of the existence of the license.

A legal thinking should be ensured in this regards along to the consideration of the necessity to maintain the exemptions in a digital environment. HUGENHOLTZ has drawn a useful categorisation of the copyright exemptions. The first category aims at safeguarding the fundamental rights of the users such as freedom of expression and information and right to privacy. The second category of exceptions reflects various public interest considerations. And finally, there are the market failure exceptions which result from a lack of possibility to control some exploitations of the works.

This could constitute a good basis for such a consideration, even if long discussions would be needed to classify the existing exceptions in one category or another. And maybe the categorisation would not be the same from a country to another since the public and general interests could largely vary. At least , the market failure should be the same across the national borders.

Harmonisation of the exclusive rights of the author and the limitations in the networked environment will constitute a distinct advantage for ERMS developers who will be able to build in to their ERMS these requirements. However, such requirements will only be taken into consideration by developers in so far as they are binding in the sense that they will not be overridden by contract and therefore by an ERMS.

Suppletive exceptions could perhaps be included in ERMS, depending on the bargaining power of the negotiating party. Libraries could simply refuse to use a technical system of protection that does not allow the free browsing by its registered users.

5.2. The imperative exceptions in the law

a. the European regulatory framework

At present the binding nature of copyright exceptions is not unknown since the database and software directive provide that some exemptions are imperative.

Article 6 of the database directive concerning the exceptions to the restricted acts says that « *The performance by the lawful user of a data base or of a copy thereof of any of the acts listed in article 5 which is necessary of the purpose of access to the contents of the data base and normal use of the contents by the lawful user shall not require the authorisation of*

the author of the data base. Where the lawful user is authorised to use only part of the data base, this provision shall apply only to that part ».

Article 8 (Rights and obligations of lawful users)is also mandatory: *« The maker of a data base which is made available to the public in whatever manner may not prevent a lawful user of the data base from extracting/and/or re-utilising insubstantial parts of its content, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Where the lawful user is authorised to extract and/or re-utilise only part of the data base, this paragraph shall apply only to that part »....*

This article means that ERMS developers who wish to protect a data base that can benefit from the sui generis form of protection will have to define with the beneficiaries of the protection what is to be considered as an insubstantial part and allow this part to be used freely. It would seem that this is somewhat difficult to exercise .

In any event, it has also become certain that only Articles 6(1) and 8 are binding in the sense that any contractual provision contrary to these articles shall be null and void[69]. It has thus become obvious that the only binding or positive rights for the lawful user of a data base is the right to extract or re- utilise insubstantial parts of the contents of the data base, for any purposes what so ever and the performance of any of the restricted acts which are necessary for the purposes of access to the contents of the data base and normal use thereof. All the other exceptions to the restricted acts are not binding and can be restricted by contract, and thus by technical systems of protection.

On the other hand, the article 5 of the software directive provides for a limited number of restricted acts. The article provides that the authorisation of the right holder shall not be required to reproduce permanently or temporarily the computer program where such acts are necessary to use the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction. It is also said that such is the case, in the absence of any specific contractual provision providing otherwise. A contract and therefore a technical system of protection could control such acts. This is a clear provision for an ERMS developer.

The making of a back-up copy by a contract is also listed as an exception in the software directive. This exception may not be prevented by contract and therefore by a technical system of protection

Articles 5.3. and 6 (Decompilation) do not specify whether they are of a binding nature or not.

---

69 Article 15 of the Directive

b. The particular case of the Belgian Law

The Belgian Law transposing the database directive has modified the Copyright Act or 'Loi sur le Droit d'auteur' of the 30d June 1994 in such a way that all exceptions to the copyright and related rights are considered as imperative and can not be overruled by contract.

Indeed, the transposition law has enacted a new article 23bis stating that the provisions of articles 21, 22, 22bis and 23§ 1 and 3, (these are the articles containing the list of exceptions) are of binding nature. The same is said as regards the exceptions to the neighbouring rights[70].

The rationale behind this surprising decision is that the legislator have regularly noticed, namely in the negociations with the rightholders as regards the remuneration for private copy levy, that the rightholders wanted to negociate the amount of the remuneration for levy systems by contracts, which could result that the exception is void of meaning..

Rather surprisingly, such a provision has passed the voting process without any deep discussion.

Even if we consider that such a reflexion should take place in any European Country, the Belgian process has been pretty rapid. There has not been a rough debate nor a deep consideration. Moreover the provision is general and covers any type of exception. We think that a proper consideration should be ensured for each exception as regards its rationale, its scope, the possible effects for the rightholders, the consequence in a digital world, and the effective difficulty of the exercise of the exception. All the exceptions should not deserve the same treatment.

This Belgian particularity has also covered the private copy exemption. Yet, this last one is certainly the most discussed one as a strong debate and opposition has been raised recently. Indeed it has been argued that, since technology can now prevent and control the making of copies, the rationale behind this exception, i.e. the market failure, does not exist anymore.

Such idea appears in the Proposed Copyright Directive which states in its recital 27 that the technological measures are entitled to inhibit the making of a private copy. It indicates that the European Commission considers this private copy exception as non binding. If the text of the Directive does not change on that point, and if the recitals are regarded as in force, the Belgian Law should be changed so as to qualify the private copy as only suppletive.

---

70 art. 26 of the transposition law enacting an article 46.3° bis in theBelgian Copyright Act.

5.3. Consequences of the binding nature of some exceptions for the ERMS

In the Copearms project, the partners and the vertical consortia we have assisted are pretty aware of the issue of the copyright exceptions. In most cases, they do not want to neglect or override the exceptions. Anyway, the legal uncertainty around the nature of the exemptions can entail a number of difficulties in the design and operation of the ERMS. Therefore, at present, the systems developed do not enable a proper exercise of exemptions. The reason why is that the technology can not easily comply with the exercise of exceptions. Indeed , what the ERMS inhibit is the making of a reproduction act or communication act. Many exceptions consist of authorising reproduction or communication for certain legitimate purposes. The technology and the ERMS can not check the effectiveness of this purpose. The technology is blind in that respect. It cannot verify whether the requested reproduction is made for a criticism purpose and in the limits imposed by the law. The only thing they can detect is the making of a restricted act.

Therefore, providing for the binding nature of the exceptions would not be sufficient. Adapted solutions should be found so as to enable Information Society services wrapped in technological protection measures to take into account a legitimate exercise of exceptions.

Two cases should be distinguished:

Firstly, the technology encapsulates a copy of a protected work.

In this case, nothing prevents a user from enjoying exceptions in other copies of the work. Nevertheless, a lawful user which could be defined as a user having lawfully access to the protected work (for instance an authorised end-user in the Cited Reference Model) should be able to accomplish some acts of reproduction or communication, as permitted in the analogue world. He should be allowed to make a reproduction or communication for criticism, research, education purposes, etc. The notion of a lawful user should be the same than that provided in the database directive.

Secondly, the technological measure encapsulate the only available copy of the work. It could be the case, for instance if the work has been created in a digital form for the purpose of the copyrighted application protected by the ERMS. Databases of digital information will generally be included in this case. The rightholders regularly compare this situation with that of the museums that can ask a remuneration for the access to the works. We think that it is

not a good example since when a visitor goes inside a museum, he does not exercise any copyright exception as regards the work. Even if he would like to do it , he could to some extent. Nothing prevents a visitor to make a copy of a work (the example of the prohibition to photograph a work is another bad one, as this prohibition is in most cases justified by conservation objectives). In the case of technological measures, both the access and the possibility to make a reproduction of a work are restricted.

On one hand, a legitimate access to the works should be granted to the public, but this a public policy matter. The legislator could and should consider this priority issue in order to avoid a world of cultural and informational content locked in technical systems. Some ideas have already been stressed such as the setting-up of a register where the works should be deposited in order to ensure a free or low-cost access for the public. This could constitute a sort of universal service in the field of the providing of cultural and informational content. The same concern is particularly true with the public domain which could be locked in a protecting technology.

But even for the users enjoying the access to the copyrighted application as a whole, they could be prevented from exercising an exception in the works components of the application.

This is the real issue of the development of technological measures. As we have seen earlier, it does not suffice to provide a binding nature of the exceptions since the technology by its very nature will not be able to comply, in most cases, with such an imperative nature. We could envisage the example of the imperative exception provided in the database directive as regards the right for the lawful user to extract and re-utilize a non substantial part of the database. The ERMS should comply with that provision and allow the user to extract a non substantial part of the database. But, since the notion of substantial is qualified quantitatively and qualitatively, the technological system is not capable to check whether a part extracted by an user is substantial or not. The only way to do it is to design the ERMS in such a way that some parts of the database protected are qualified by the rightholders as non substantial. This unilateral decision could make the exception void of meaning.

Some other ways to comply with the exercise of exceptions should be considered such as an obligation to provide an alternative copy of a work at low-cost or for free to any person wanting to exercise an exception or a general licensing scheme in some sectors which could grant a reasonable exercise of exceptions. This could be done for instance with the libraries, in the educational sectors or in with any other large collective users. Nevertheless, we do not envisage at present a perfect solution for arriving an acceptable balance between the rights of the rightholders and the users.

5.4.Conclusion

This matter of the exceptions and public domain versus a misappropriation by technological measures is certainly the hottest topic of this deliverable and of the current discussions on the future of copyright. It is also certainly the most difficult one.

The copyright has always dealt with the restricted acts of reproduction and communication. In the Information Society a most important feature could be the access to the works. The access is a notion of a market where the access to a protected content is a service to sell and to buy. It is not and it should not be a matter for copyright. Therefore a remuneration of the access could be justified but this could not be the basis for preventing the users from exercising some legitimate exceptions in the works to which they get access. Nevertheless, since the technological measures and this is the case for ERMS both protect the access and the reproduction or communication of the works, the boundaries of the restricted rights seem less and less limited.

As a conclusion, a legislative consideration should be taken on one hand as regards the access to public domain and more generally to cultural content in the Information Society; and on the other hand on the nature of copyright exemptions and the possibility to override them by contract or by a technology such as an ERMS.

6. LEGAL PROTECTION OF ERMS*

6.1. INTRODUCTION

A proper protection of technical devices such as ERMS, against circumvention is a prerequisite for their economic development, and thus for IPR management in the Information Society. As soon as technology has been envisaged to enhance an effective exercise of copyright, it has been feared that a similar technology might be used to defeat the technical protection. Therefore a due protection of the electronic copyright protection and management systems has always been a great concern of the rightholders and of the industry developing these systems.

The WIPO Diplomatic Conference of 1996 has considered this issue as a priority field for action. As a result, the Members of WIPO will have to stress the legal protection of technical measures by implementing the WIPO Treaties in their national law. The European Union and the United States have already prepared and proposed pieces of legislation aiming, amongst other things, at taking a due account of this important development of copyright management. All the initiatives are based upon a prohibition of circumvention and preparatory activities to be enacted in the Copyright Acts.

Another important development of the digital technology as regards the IPR protection is the digital information systems enabling a proper identification of works, rightholders and digital support. These identification systems, such as that developed by the CISAC or the DOI developed by the Association of Publishers, need to be protected against any removal or alteration. Therefore, the WIPO Treaties and the Proposals hereabove mentioned have equally provided a legal protection prohibiting the defeating of the so-called 'rights management information'. We will see that the definition given to these Rights Management Information could cover ERMS as well.

* Author : Séverine DUSOLLIER. This part of the deliverable if particularly long. We have considered that this issues was very specific to the development of ERMS and deserved a peculiar attention since this new issue of the protection of the technology and its consequence have not been in-depthly addressed yet.

6.2. EXISTING PROTECTION OF ERMS

a. Software Directive

The software directive of 19 May 1991[71] is the first piece of enabling legislation which has ever provided a legal protection of anti-copy devices. The protection contained herein should be similar in Member States legislations having transposed the Directive.

The relevant provision which could be used to protect technical systems of protection in so far as they protect computer programs is the Article 7 1. (c) of the software directive which states that *"... Member States shall provide....appropriate remedies against a person committing (...) c) any act of putting into circulation or the possession for commercial purpose of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program."*

As far as we know, only German case law[72] has ever dealt with that provision. Indeed, the German Supreme Court has stated that in order to apply the criteria of the 'sole intended purpose', it is not the purpose of the program enabling the circumvention which has to be considered but rather the purpose of the application itself. Therefore, a program being capable of other features than the mere circumvention of a technological measure might be prohibited if the sole purpose of one application thereof is aimed at circumventing. The criteria of the Directive has thus been largely construed.

A soon as the Proposed Directive on harmonisation of certain aspects of copyright[73] will be adopted, this protection should be modified so as a harmonised level of protection could be applied to all types of works and prestations.

b. The protection of ERMS as a Software

An ERMS can be a computer program protected as such by the Software Directive. It is the case of theCopicat and Copysmart Software applications for instance. Is the protection granted by the Directive sufficient to protect the ERMS against any circumvention or defeat ?

---

71 Directive 91/250/CEE , JO L 122/42, 17.05.91

72 M. LEHMANN. German Report. ALAI Study days. June 1996, Otto Cramwinckel. 1997. p. 367.

73 Proposal for a European Parliament and Council Directive on the harmonisation of certains aspects of copyright and related rights in the Information Society. 10.12.1997, COM(97)628 final. hereafter 'the Proposed Copyright Directive'

By virtue of the Directive, the rightholder enjoys from a exclusive right to authorise the reproduction, adaptation and any other alteration of a computer program. In the course of the act of circumvention, an adaptation or reproduction might occur. Equally, in the manufacture of circumvention devices, a reproduction or adaptation of the software to be circumvented can take place.

Nevertheless, the protection granted by the Directive on computer programs is limited to the case where the ERMS itself is a software and where the circumvention activities presuppose a reproduction thereof or any other restricted acts. Moreover, other technical protection measures might not be protected by this provision. And last, but not least, the protection shall only be enjoyed by the author of the ERMS, thus the person or company having developed it. The rightholders using it for protecting their works won't be entitled to prohibit the reproduction of the computer program.

In conclusion, the protection by this Directive, at least by the general rules of copyright and not by the special protection provided by the article 7 of the Directive, appears to be inappropriate.

Yet, in a US case law[74], a plaintiff has evoked this protection. The facts of the case were the following: Vault had developed a software protecting other software against unauthorised copy. Quaid developed a software product enabling to undo Vault's system. Vault sued Quaid for direct infringement[75] on the basis that Quaid had probably made an infringing reproduction of Vault's software so as to learn its way of working before developing its circumvention device. This argument was overruled since such a reverse engineering can be qualified as fair use. This judgement wouldn't be the same in Europe where the reverse engineering exemption is valid upon strict conditions. Indeed, the decompilation exemption provided by the Directive, should not be of application in this case since this exemption requires that the decompilation is made to achieve the interoperability. Of course, the decompilation of an ERMS should not be permitted for the purpose of designing a circumvention device.

c. Protection by other civil rules

The manufacture, sale or any other act of distribution of circumvention devices could be inhibited by evoking a contributory infringement to copyright. This has namely be done in

---

74 Vault v. Quaid. 655 F, (5th Circ. 1988)

75 There were also other grounds for the action, see SAMUELSON, 1996. Technological protection for copyrighted works. available at <http://www.sims.berkeley.edu/~pam/courses/cyberlaw/docs/techpro.html>

the US[76], albeit with no success. Two US judgements held that since the device can carry out any other substantial non infringing use, besides the circumvention of technological protection measures, the manufacturer of this device should not be contributory liable.

In Europe, a German decision[77] has held contributory liable the provider of the means to copy, upon the condition the device was intended for a use which could normally infringe copyrights.

A problem can be raised by the use of liability rules which requires the proof of a damage. What is the actual damage suffered by the rightholder when circumvention devices are manufactured and sold ? The damage in this case is only future and contingent. Nevertheless, the common liability rules could help prohibit devices which are specifically and intentionally designed for circumvention purposes, by default of anti-circumvention legal protection.

Other case law have outlawed circumvention devices on the ground of competition law or unfair commercial practice[78] or on grounds on computer crime legislations[79].

6.3.LEGAL INITIATIVES FOR PROTECTING TECHNICAL MEASURES

a. WIPO TREATIES

On December 20, 1996, the Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions[80] adopted the «WIPO Copyright Treaty» (WCT) and the «WIPO Performances and Phonograms Treaty»[81]. (WPPT)

---

76 SAMUELSON , ibidem , p. 6-8

77 OLG Muenchen, 07.12.1989, AZ 29 U 5482/89 ("Firma Teleclub") mentioned in LEHMANN, op. cit.

78 M. LEHMANN, op.cit., 1997, p. 367; W. GROSHEIDE, Dutch Report, ibidem, p. 403

79 N.A. SMITH, US Report, ibidem, p. 422. W. GROSHEIDE, op. cit., p. 408

80 Referred to below as the diplomatic conference

81 available at <http://www.wipo.org>, referred below as WIPO Treaties.

In the field of the provisions on the protection of anti-circumvention devices, the discussion was very controversial. Before the Diplomatic Conference, the US had proposed a text which goes along the lines of the text proposed in the White Paper (see below). The European Community and its Member States have submitted the following proposal:

> *«Contracting Parties shall make it unlawful, and provide for appropriate remedies against, the manufacture, distribution and possession for commercial purposes of any device, means or product, by any person knowing or having reasonable grounds to know that it primary purpose or primary effect is to remove, deactivate or circumvent, without authority, any process, mechanism or system which is designed to prevent or inhibit the infringement of any of the rights under the Berne Convention or this Protocol.*
>
> *«Contracting Parties shall make unlawful, and provide for appropriate remedies against, the offer or performance of any commercial service, by any person knowing or having reasonable grounds to know that its primary purpose or effect is to remove, deactivate, or circumvent, without the authority any process, any mechanism or system which is designed to prevent or inhibit the infringement of any of the rights under the Berne Convention or this Protocol».*

On 30 August 1996, the Chairman of the Committees of Experts on a Possible Protocol to the Berne Convention and a Possible Instrument for the Protection of the Rights of Performers and Producers of Phonograms submitted a provisional copy of the basic proposal for the substantive provisions to be included in the treaty. This document contained an article82 on the «Obligations concerning Technological Measures» which provides that:

> *«(1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this treaty that is not authorized by the rightholder or the law.*
>
> *(2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).*
>
> *(3) As used in this article, «protection-defeating device» means any device, product or component incorporated into a device or product, the primary purpose or effect of which is to circumvent any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty».*

---

82 Article 13.

Some countries[83] and interest groups have expressed such a strong opposition to these proposals at the last meeting in Geneva[84] that the text finally adopted states simply :

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

A similar text appears in the WPPT.

This formulation is very large and does not specify the type of protection Contracting Parties shall provide, neither the definition of protected devices. Therefore, it will be a matter for national laws to implement a detailed protection. Consequently, the protection might not be harmonised.

c. European Regulatory framework

i. Green Paper and Follow-Up

The Green Paper on Copyright and Related Rights in the Information Society[85] (referred to below as the Green Paper) stressed the need to develop technical systems of protection and identification if the information society is not to operate to the detriment of right holders[86].

This view was reiterated numerous times during the hearing which was organised by the Commission on 8 and 9 of January of 1996 on technical systems of identification and protection and on the acquisition and management of rights. A majority of participants also indicated that although such systems should not be made compulsory, some felt that legislation should be put in place so as to ensure effective application of the systems. The acts of circumventing, violating or manipulating these systems should be made subject to

---

83 Such as Norway and some African States.

84 Committee of experts on a possible protocol to the Berne Convention, seventh session and Committee of experts on a possible instrument for the protection of the rights of performers and producers of phonograms, sixth session. Geneva. May 22 to 24, 1996.

85 Brussels, 19.07.1995, COM (95) final.

86 Green paper, page 79.

sanctions, whether civil and/or administrative or even criminal. Harmonisation at an international level was requested.

Namely based on this consultation process, the European Commission issued a so-called Follow-up to the Green Paper on Copyright and Related Rights on 20 November 1996[87], in order to set out the Commission's policy in this area which stresses, among others, the intents of the Commission in the field of the technical identification and protection schemes, considered as a priority issue. With a view to arriving at interoperable systems, the Commission seeks further pursuing of the standardisation work in this area.

In the Follow-Up, the Commission indicated that the envisaged protection should take a due account of a precise definition of the scope of protection and the nature of the appropriate sanctions, the properties of the protecting device, the nature of the act to be covered (such as manufacture, possession in the course of business, putting into circulation, distribution, importation), the way or process of circumventing / deactivating, users' rights, the scope of the infringer's liability and possible legitimate defences, etc. It should also be ensured that systems are designed in a way which respects the right to privacy with regard to the processing of personal data.

ii. Proposed Directive on Copyright

Following the intention of the Follow-Up, The Commission has addressed in its recent Proposal for a Directive on certain aspects of copyright and related rights in the Information Society[88] the matter of the legal protection of electronic management and protection systems as follows :

> Art. 6 : "*Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices or the performance of services, which have only limited commercially significant purpose or use other than circumvention, and which the person concerned carries out in the knowledge or with reasonable grounds to know, that they will enable or facilitate without authority the circumvention of any effective technological measures designed to protect any copyright or any related rights*".

---

87 Communication of the Commission on the Follow-Up to the Green Paper on Copyright and Related Rights in the Information Society, COM(96) 568 final, 20/11/96.

88 COM(97)628 final, 10.12.1997Reffered to below as "the Proposed Directive on Copyright",

This text aims explicitly at transposing the WIPO Treaties of 20 December 1996[89].

iii. Proposed Directive on conditional access

The proposal for a directive on the protection of conditional access[90] might constitute a basis for preventing the circumvention of technical devices blocking the access to information services, since the scope of this proposed piece of legislation covers pay-TV, video-on-demand, electronic publishing as well as a wide range of on-line services.

The explanatory memorandum and recitals for this directive excludes the circumvention of rights management information and the technological measures used by the authors in connection with the exercise of their rights[91]. However, the protection granted by both Proposed directives could easily overlap and particularly for the services protected by an ERMS. Indeed, such a system is generally designed both to control the access to a information service as a whole and to monitor the usage of the IPR-protected content. A clear distinction between these main features of an ERMS would be difficult to draw and this will be particularly true in the future since the convergence between the broadcasting services and the telecommunications brings a greater confusion between services and content as well as between the actors and the roles they play in the Information Society.

We will deal with this contradiction later on. For now, suffice it to say that the directive provides that *"Member States shall prohibit on their territory, each of the following activities:*

- *the manufacture, import sale or possession for commercial purposes of illicit devices;*
- *the installation, maintenance or replacement for commercial purposes of an illicit device;*
- *the use of commercial communications to promote illicit devices",*

whereas the illicit devices are defined as any equipment or software designed or adapted to enable the unauthorised access to a protected service.

---

89 Explanatory Memorandum, n°10; Background to the Proposal.
<http://europa.eu.int/comm/dg15/en/intprop/1100.htm>

90 Proposal for a European Parliament and Council Directive on the Legal Protection of Services based on, or consisting of, Conditional Access, COM(97) 356 final, 9.7.1997. available at <http://www2.echo.lu/legal/en/converge/condaccess.html>

91 Recital 15

c. US POSITION

A few years ago, the US White Paper[92] had already recognised that "the ease of infringement and the difficulty of detection and enforcement will cause copyright owners to look to technology, as well as the law, for protection of their works"[93]. It was also emphasised that technological protection will not be effective unless the law provides some protection for systems used to prevent or restrict unauthorised uses of works protected by copyright.

The Working Group recommended that the US Copyright Act should be amended so as to include a new chapter containing a provision to «prohibit the importation, manufacture or distribution of any device, product or component incorporated into a device or product, or the provision of any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights under section 106».

Such a protection was not unprecended in the US legislative framework that contains the Audio Home Recording Act (17 USC §1002c) and section 605 of the US Communications Act (47 USC § 605) which regulates devices enabling the decryption of television programmes transmitted by satellite. The Audio Home Recording Act provides for an obligation to integrate in any digital audio recording device a Serial Copy Management System, while prohibiting the circumvention of such systems. Nevertheless, the scope of this prohibition was limited to a specific and precisely defined technology[94] and the technology itself was not aimed at blocking access to a work nor preventing the making of one copy95.

After a strong influence on that point during the adoption of the WIPO Treaties, new Bills for implementing the WCT and the WPPT have been recently proposed . Many of these Bills deal with the protection of technical measures against circumvention. The Bill 2281, so-called the 'Digital Millennium Copyright Act of 1998'[96], considered as being the closest Bill to the US Administration views has recently been passed by the House of the Representatives

---

92 Report of the Working Group on Intellectual Property Rights on Intellectual Property and the national Information Infrastructure, Referred to below as the «White Paper».

93 See White Paper, p. 230.

94 T. VINJE, "A brave new world of technical protection systems : Will there still be room for copyright ? ", EIPR 1996, n°8, p. 431., p. 432

95 SAMUELSON, op. cit.

96<http://www.aop.org/legis/wipo.html >

on the 4th of August. This is the reason why we will focus on that Bill. Some changes might be probably made to this text since this Bill and the one approved by the Senate this past April are to be worked out in a House/Senate conference committee before going back to both chambers for approval

This long and sometimes intricate text provides a twofold protection, one for the access to protected works and the other for the protection of the copyright owner's rights, as follows:

> *(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES-*
>
> *(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.(...)*
>
> *(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--*
>
> *(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;*
>
> *(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or*
>
> *(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.*
>
> *(b) ADDITIONAL VIOLATIONS-*
>
> *(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that*
>
> *(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;*
>
> *(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or*
>
> *(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.*

6.4. The scope of the legal protection of technological measures

It appears from the different legal provisions mentioned above that the envisaged protections are often pretty various, even contradictory in some cases. The main differences are exposed below in terms of the object of protection, the definition of prohibited acts and of illicit devices or services, the requirements for such a prohibition, the type of sanctions and the consideration of copyright exemptions and limitations.

a. Object of the protection and definition of technical measures

The scope of the protection of all these existent or to-be legislations is pretty similar, albeit a large range of definitions applying the relevant provisions of the WIPO Treaties.

The WIPO Treaties addressed the "*effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works which are not authorised by the authors concerned or permitted by the law*". The precise definition of the technological measures to be protected has been left to the national laws.

The Proposal for a Copyright Directive aims at protecting the " *effective technological measures designed to protect any copyright or any related rights defined as : any device, product or component incorporated into a process, device or product designed to prevent or inhibit the infringement of any copyright or any rights related to (...)*". The technological measures shall only be deemed effective -and as a consequence covered by the protection- "*where the work or other subject matter is rendered accessible to the user only through application of an access code or process, including by decryption, descrambling or other transformation of the work or other subject matter, with the authority of the rightholder*" (emphasis added).

According to the Explanatory Memorandum, this definition of the 'effectiveness' of the measure entails that the rightholders have a duty to demonstrate the effectiveness of the technology chosen in order to obtain protection[97]. But we are still puzzled as regards the presumption stated by this provision which states that the effectiveness shall only be deemed upon the condition that the object of the technical protection is the access. Does it mean that the rightholder escapes to the burden of the proof in all cases where the technical measure relates to the access to works or other subject matters ? As a consequence, the protection

[97] Comment on article 6.

against its circumvention shall be automatically granted , whilst in all other cases (for instance, where the access is free, but the reproduction, printing or further communication is inhibited by the technological measure), the rightholder has to prove the effectiveness of the chosen measure. Another way to put it is that the effectiveness of the measure shall only be met where it relates to the access. In this case, how will be protected the technical devices granting a free access while monitoring the usage of the protected content ? Given the word 'only' in this sentence, we would be inclined to consider that the second meaning prevails. Should it be true, some technical measures would not be protected by this Directive. For instance the Serial Copy Management Systems, or the mere anti-copy devices, or even some ERMS which would be designed or programmed only for usage-tracking purposes. This is not only a theoretical case. The flexibility of ERMS such as the Cited Model, enables various scenarios in terms of access and protection of works. For instance, a library or a school could give access to a collection of works with the authorisation of rightholders upon the condition , subject to a technological protection, that its pupils or its visitors are not allowed to copy , print or communicate the work to other people. In this case where the access is not the main objective of the technological measure, would it be still entitled to enjoy from the protection ?

Such a consequence of this text would not be of course a good thing. Therefore, the wording of this definition of the effectiveness of the technical measure should be properly reviewed. A proper definition should define the technical measure as enabling the exercise of the rights of the rightholder rather than stressing the 'access' element.

As regards the Proposed Directive on Conditional Access, it covers "*the 'protected services', the provision of which are provided on the basis of 'conditional access' as well as the provision of conditional access to the above services as a service in its own right*", whereas "Conditional Access" means *any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon prior individual authorisation aiming at ensuring the remuneration of that service.*

The envisaged "*protected services* " could be television and radiobroadcasting services as well as Information Society Services, e.g. video or audio-on-demand, electronic publishing, on-line access to a database and a wide range or other on-line services, all of which are offered to the public on a subscription or usage related basis. The key element is thus that the access to the service is made conditional upon a prior authorisation aiming at ensuring the remuneration of the service. The remuneration does not need to be prior to the access nor a lump sum. This means that systems which both enable the access and send an invoice related to the actual usage, such as ERMS, are entitled to this protection. The provision of such ERMS would be considered as a service in its own right, as mentioned in the Proposal. The main difference with the Proposed Copyright Directive is that it refers to the access to a service whilst the latter refers to the access to works or other subjects matters . The only case where both protections are entirely overlapping is the on-line access to a database where the

service is itself the protected matter.

Another key difference has to be highlighted : in the Conditional Access, the remuneration of service providers is the protected interest while the Copyright Directive aims at protecting the rightholders. Anyway, in most cases of on-line exploitation of IPR-protected content, the service provider might be the rightholder, for instance the database rightholder, the producer or the publisher. Moreover in the case of ERMS, the service provider protects its service by this system for his own interest and monitor usage of works on behalf of rightholders.

The criteria of remuneration is not either sufficient to draw a clear distinction between conditional access and technological measures since the remuneration managed by the ERMS can consist of payment both for access and for copyright licences or royalties. Besides, for taxation reasons, the remuneration can be deemed by the service provider as a royalty only which in many cases benefit from a lower rate of taxation.

Only to mention it, the scope covered by the art. 7, 1 (c) of the Software Directive was the *technical device which may have been applied to protect a computer program*. The 'protection' was not further defined.

Finally, the US Bill aims at ensuring the protection of technological protection measure which either "*effectively controls access to a work protected*" , either "*effectively protects a right of a copyright owner or a portion thereof*".

It is said further that on one hand, the technological protection measure effectively controls access to a work if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the rightowner, to gain access to the work; on the other hand the measure effectively protects a right if the measure, in the ordinary course of its operation, prevents, restricts or otherwise limits the exercise of a right of a copyright owner. (emphasis added)

This twofold protection appears pretty complicated, more especially as the violations regarding the circumvention are very similar. The only key difference is that the circumvention itself is only prohibited as regards the technological measures granting access to works. This difference has no evident justification. Moreover the wording used to characterize the effectiveness of the second type of measure (protection of a right) is somewhat confusing. Indeed, the purpose and effect of technical protection measure is not to prevent, restrict or limit the exercise of the copyright but rather to enhance it. What is limited or prevented is the exercise of acts of exploitation restricted by the copyright law. Whatsoever, since many technological measures can both control the access and protect the rights, a separated protection seems not justified.

b. Object of the sanctions :

Illicit devices or services :

The Proposal for a Copyright Directive seeks to prohibit the devices or services, which have only limited commercially significant purpose or use other than circumvention . The software Directive refers to any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device . As regards the protection of conditional access, the prohibition covers the illicit devices which are defined as any equipment or software designed or adapted to enable the unauthorised access to a protected service. (emphasis added)

The US Bill refers to any technology, product, service, device component, or part thereof that (A) is primarily designed or produced for the purpose of circumventing a technological protection measure or (B) has only limited commercially significant purpose or use other than to circumvent a technological protection measure. (emphasis added)

These standards for the illegitimacy of the device or service vary largely from a text to another. The concern was to draw a clear line amongst the electronic and technological devices between those whose circumvention is one of their explicit or envisaged purpose and those which can incidentally circumvent a technical protection measure. The electronic consumer manufacture industry is particularly concerned and wish to prevent their products being outlawed only because they can be used by their users for circumvention purposes. The level of circumvention features as regards other main features of the product is also relevant. For instance, if a video recorder can be used to bypass an anti-copy device, while its main objective is to play and record videotapes, does it mean that the videorecorder has to be considered as illicit ?

The first criteria used in the US White Paper was the 'primary purpose or effect' , which could prohibit devices used beyond the intention of the manufacturer for circumvention purposes. The White Paper faced a strong opposition on that point[98]. As a consequence, the current legal initiatives limit the forbidden devices whose purpose is mainly the circumvention.

We are wondering anyway how the "limited commercially significant purpose or use" will be construed. Will a device primarily designed and sold to accomplish a legitimate purpose but being eventually largely acquired because of a circumvention use, be considered as

---

98 SAMUELSON, op. cit.; VINJE. op. cit.

illicit? What is commercially significant ? Is it 51 % of licit use, 75 %, 30 % ? Could a device be outlawed in one country while being licit in another ?

Nevertheless, since the 'effect' has been definitely removed from any text, the criteria of the 'limited commercially significant purpose or use other than the circumvention' should be considered as a reasonable and appropriate one, even if the notion might be construed very differently from a country to another.

Illicit Activities :

A number of activities shall be considered illicit as regards the circumvention of technical protection measures. According to the Proposed Copyright Directive, any activities, including the manufacture or distribution of devices or the performance of services, that facilitate or enable the circumvention shall be prohibited. As regards the conditional access, the installation, maintenance or replacement for commercial purposes of an illicit device; the use of commercial communications to promote illicit devices; and the manufacture, import, sale or possession for commercial purposes of illicit devices.

The Software Directive refers to any act of putting into circulation, or the possession for commercial purposes.

The US Bill prohibits the circumvention, the manufacturing, importation, the offer to the public, the providing or any other traffic, as well as the marketing.

All these lists are very large and aim at preventing any commercial exploitation of an illicit device. As the Memorandum of the Proposed Copyright Directive states, the real danger for IPR will not be the single act of circumvention by individuals, but the preparatory acts carried out by commercial companies that could produce, sell, rent or advertise circumventing devices. Yet the act of circumvention in its own could be outlawed by the envisaged legal provisions. For instance, the US text considers explicitly the circumvention itself as an infringement to which an individual user could be held liable, albeit only in the case where the measure controls the access to a protected work. This restriction to the first type of protection granted by this Bill has no explicit justification. From our point of view, the act of circumvention itself might be prohibited as well by the Copyright Directive which refers to 'any activities'. The text should make it clear whether the circumvention itself is covered by the prohibition or not.

The rationale of all these texts is to prevent preparatory activities, such as the manufacture, distribution, promotion, rather than the mere act of circumvention. This seems justified since the act of circumvention will lead to a copyright infringement (except in the

case of the exercise of an exception) which will be in itself prohibited. As a consequence, the sanction of the copyright infringement should suffice. No other sanction should be applied. At the contrary, providing means on a commercial scale to bypass the technical protections is still not covered by the scope of copyright protection. This justifies the envisaged prohibition.

The Proposed Copyright Directive and the US Bill explicitly consider that the performance of services may be considered illicit. However, since the software Directive refers to 'any means' , the services are covered by all the texts, but the Proposed Conditional Access Directive. It is particularly relevant to cover the prestations of services, since in a near future, the on-line providing of software or any other circumvention devices might be considered as services, namely for VAT purposes[99].

Liability requirements

As we have seen earlier, a number of criticisms have raised in the first attempts to prohibit the manufacture of circumvention devices or at least of devices which can be used for circumvention, even if it was not their primary purpose[100]. The idea then developed was to hold liable the manufacturer or distributor of infringing products or devices only if he had a knowledge of the possible circumventing utilisation.

This element can be found in the Proposed Copyright Directive that limits the liability to the acts that the person concerned carries out in the knowledge or with reasonable grounds to know, that they will enable or facilitate without authority the circumvention of any effective technological measures. Such a limitation of liability does not appear in the Software and Conditional Access Directives . Recently the common position of the Council and Parliament on the Conditional Access Proposed Directive suggested to introduce a possibility for Member States to provide a knowledge element when transposing the Directive[101].

At the contrary, the knowledge element appears in the US Proposal although it is only required for the marketing activity,

This element can reasonably limit the uncertainty resulting from the criteria of 'limited commercially significant purpose'.

---

99 See Communication of the Commission

100 VINJE. op. cit.,

101 Common Position, JO 19/8/98, C 262/36. recital 21

c. Exceptions and public domain

We have seen elsewhere[102] that the question of the possibility to override copyright exemptions is a particular concern in the field of technical measures such as ERMS that can inhibit a proper exercise of a large range of exceptions and wrap public domain material. At present, this question has been considered in a twofold way. On one hand, the legislative bodies can state that some exceptions are of binding nature and are not to be contracted around or denied by technical protection. We have seen the little reluctance to decide upon this matter so soon, with the exception of the Belgian Law.

On the other hand, one can consider that the protection of technical measures has to take into account the exercise of copyright exemptions by not outlawing the circumvention measures which are made or designed in order to exercise such exemptions. This has been unclearly done in the WIPO Treaties that states that the protection of technological measures will be limited to the measures that restrict acts which are not authorised by the authors concerned or permitted by the law. This has been understood as providing that the exercise of exceptions should be taken in due account by the national legislators. But does it mean that the circumvention itself or the devices which enables the exercise of a copyright exemption should not be prohibited ?

Two cases should be distinguished here. Firstly, we have to consider if the circumvention of technological measures carried out by the user himself in order to exercise a legitimate copyright exemption or to get access to public domain material has to be prohibited.

We have seen above to what extent the Information Society might represent a threat for the balance of rights. A number of authors and users fear that a free access to public domain and a reasonable exercise of the copyright exemptions will not be maintained.

Facing a strong criticism on that point, most proposals we addressed here have considered this issue, albeit generally in a unsatisfactory manner.

The US Bill has a strong concern in this regards, even if the outcome is not really convincing. On one hand, the prohibition of the circumvention of technological measures controlling access to works is delayed at the end of a period of two years. During this time, the Secretary of Commerce and the Register of Copyright shall conduct a rule-making so as

---

102 Title II. 5. of this deliverable

to determine the effects of the prohibition on non-profit libraries, archives, educational institutions as well as on persons having gained initial lawful access to works. This rule-making will consider "whether users of copyrighted works have been, or are likely to be adversely affected by the implementation of technological protection measures that effectively control access to copyrighted works". In conducting the rule-making, the Secretary shall examine several factors including the availability for use of copyrighted works; their availability for archival, preservation and educational purposes; the impact of technological protection measures on traditional fair uses such as scholarship, teaching, and research; the effects of circumvention of technological measures on the market for or value of copyrighted works; and such as factors as the Secretary and others consider appropriate. If the Secretary finds that an adverse impact is demonstrated or is "likely" on any particular class of copyrighted works such as journal articles, this class would be exempt from the prohibition on circumvention for the following two years to permit "lawful uses."

The Secretary in consultation with the Register and others shall renew this rule-making every two years and evaluate the waivers of certain classes of works, if applicable.

The rationale behind this provision is clearly to enforce the prohibition on the act of circumvention itself only if it does not adversely affect the exercise of users' rights and copyright exemptions. The adopted solution appears to be somewhat questionable since a possible outcome of the rule-making will be to exempt from the prohibition the circumvention to get access to certain class of works. Indeed, in most cases, the circumvention will be accomplished to get access to the information services as a whole and not to a particular type of works. Moreover, this delay of the effectiveness will only apply to 'access' type of technological measures.

On the other hand, in its section 1201 (d) (1), the Bill states , as a matter of principle, that "*nothing in this section shall affect rights, remedies, limitations, or defences to copyright infringement, including fair use*". This article appears at first sight, exempt from the prohibition the circumvention accomplished in the sole purpose to exercise a fair use. Actually, what is concerned is the defence to copyright and not to the circumvention act. It means that in the case where a circumvention took place with a view at getting access to works in the framework of fair use, the infringement of copyright might be argued and removed while the offence of the circumvention still subsists and can be prosecuted. This means that an user may sustain a sanction only for the circumvention act even if he has committed no copyright infringement. This raises the question of the actual rationale of the protection of technological measures: is it really the threat to copyright or is it rather a protection of the investment devoted to the development or the utilisation of a technological protection ? We will resume that point later on.

Finally, effective exemptions of the circumvention prohibition are provided in the US Bill for non-profit libraries and that solely in order to make a good faith determination of whether

to acquire a copy of that work and for reverse engineering purpose. The same possibility for decompilation exception appears in the Proposed Copyright Directive in its Recital 31.

For the other exemptions, the EU Proposal is not so clear. Nothing in the wording of the article 6 could be construed, in our view, to consider the protection not to cover the exercise of exemptions. However, the Explanatory Memorandum in its comment on this article, clearly provides that only the circumvention of technical means of protection which constitute an infringement of a right are covered, leaving aside the circumvention "*which are not authorised by the law or by the author*". Does it mean that circumventing a technical measure to carry out an act of reproduction or communication covered by an exception would be allowed ? If no, as we said earlier, a heavy burden is placed upon the users to exercise the exemptions they legitimately enjoy from the law. And they will be prosecuted for circumvention even if they will be considered non liable for copyright infringement.

If yes, the text itself of the Proposal should then make it clear . The wording used in the Explanatory Memorandum is neither clear as it considers whether the circumvention can be authorised by the law or not. If it aims at ensuring the exercise of exceptions, it should have referred to whether the act of exploitation upon the protected work or other subject matter enabled by the circumvention is authorised by the law or by the author. We find here the same confusion than in the US Bill.

A second point is to take into consideration the exercise of exceptions when contemplating the prohibition of what is called preparatory activities, such as the manufacture and commercial distribution of circumvention devices. It is generally considered that making available technical devices enabling circumvention of protective technical measures can help the user to exercise the copyright exemptions in a digital environment. Therefore, the prohibition of such devices should not cover the devices aiming at a proper exercise of exemptions. This limitation seems a bit inappropriate. The technological devices, and therefore the devices enabling their circumvention, prevent or inhibit the making of a reproduction act or a communication act. These acts are technology-linked, i.e. they can be identified as such by a technology. Beyond this, such technology is blind, i.e. it is not capable to distinguish amongst the accomplished acts, which are done for legitimate purposes covered by an exemption to copyright. The technology can not state whether the act of reproduction it inhibits is done for research purposes or criticism. Therefore, it seems rather unlikely that circumvention devices will be primarily designed for copyright exemptions.

Moreover, such a limitation of the envisaged protection could reduce the effectiveness of the legal protection granted for technological measures since a manufacturer of circumvention devices could easily argue that its product has a legitimate purpose, i.e. the circumvention for ensuring the exercise of an exception.

All these reasons are more justified as regards public domain material which can be

wrapped by technical devices at the same time than protected content. Technology will not be specifically designed for providing access to this type of material without enabling access to other content.

However, for the same reasons mentioned above for the act of circumvention itself, it is not clear whether the EU Proposal and the US Bill outlaw or not the circumvention devices granting the access to public domain or exercise of fair use or copyright limitations. As regards the EU Proposal, could it be argued that a device enabling the exercise of a legitimate exception *has a non limited commercially significant purpose or use other than circumvention*? We don't think so. The circumvention for a legitimate purpose is still a circumvention.

Anyway, even if we conclude that the EU Proposal exempts from its scope the distribution of devices enabling it for legitimate purposes such as the access to public domain material or exercise of fair use, such devices could be outlawed by virtue of the Proposed Directive on Conditional Access. It will suffice that the illicit device aims at granting access to Information Society Services. Any technological measures which is used to protect Information Services containing IPR content will be covered by both Directives, more especially as the definition of technological measures to be protected focuses on their 'access' feature. This is namely the case for ERMS systems. Therefore, any concern for sheltering copyright limitations in the Proposed Directive on Copyright seems pretty useless.

d. Conclusion

This question of exceptions highlights the complexity of the legal protection of ERMS and its boundaries. Either the protection does not cover the circumvention carried out for the purpose of the exercise of an exception nor the manufacture and commercialisation of circumventing devices enabling such exercise. In this case, the protection might be fragile since its prohibition can be defeated by a fair use argument and the illicit device would be easily modified so as to be considered as licit.

Either, the circumvention is always prohibited regardless the purpose for which it is carried out. In this case, the legal protection, in our view, covers rather the investment devoted to the development of the technological measure or to its use by the rightholder. It does not seem necessary then to link this protection to intellectual property regulatory framework. As W. GROSHEIDE states, "*according to their very nature, technical devices operate indiscriminately of the legal environment in which they are introduced*". The same technology will be used to protect IPR content, personal data, confidential information,

broadcasts[103], etc...

As a conclusion, we would support the view of other commentators[104] and recommend that a proper protection of technological measures against their circumvention, whatever they enable access to services as a whole, to protected content, or they monitor and manage the utilisation of protected works by registered users, should be found elsewhere than in IPR legislation. It could be done for instance by a computer crime regulation which would prohibit any unauthorised access to no free services regardless these services are copyright-based or not.

The illicit acts should be the preparatory activities such as the manufacture and commercial distribution of circumventing devices. The level of knowledge of the possible use of devices could determine the nature, either criminal either civil, of the offences. The act of circumvention carried out by an individual should be outlawed only upon strict requirements, e.g. if it has been done maliciously. In other cases, the copyright infringement which has been enabled by the circumvention should be the only basis for suing the individual.

The beneficiary of this protection should be both the service provider or rightholders if the system is used to protect copyrighted works, as well as the maker of the technological measure. The proposed provisions don't envisage clearly that he could bring an action against circumvention devices. Yet if his system can be easily defeated by a piracy device, he has a strong interest to ask for the prohibition of such device.

The ERMS should find a proper protection in such legislations, namely in the case where such systems might protect and manage copyrighted content and not-copyrighted material as well. In a near future, some ERMS could be developed in order to tackle a broader market than the IPR management and might not be entitled to the protection as foreseen by the Proposals we addressed.

Of course, in this solution, the problem of copyright limitations and public domain still subsists. But, this issue should not be dealt with at the stage of the protection of technological measures. It is too late then. The compliance of these devices with the exceptions should be ensured at an earlier stage, as early as their design and development. This could be done namely by granting to copyright exemptions a binding nature.

---

103 D. GERVAIS, Electronic Copyright Management Systems in a Network Environment, <http://www.copyright.com/stuff/ERMS_network.htm>

104 LEDGER M. & TRIAILLE J.P., Belgian Report, ALAI Study Days.

W. GROSHEIDE, op. cit., p. 403

6.5. RIGHTS MANAGEMENT INFORMATION

a. Introduction

The WIPO Treaties have enacted the first protection of rights management information aimed at protecting the new technical methods for identification of the work.

The article 12 WCT and WPPT provides :

> *"(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:*
>
> > *(i) to remove or alter any electronic rights management information without authority;*
> >
> > *(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.*
>
> *(2) As used in this Article, «rights management information» means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public. "*

b. Legal Initiatives

The European Commission as well the US Bill seek to transpose the WIPO Treaties on that respect.

The Proposed Copyright Directive requires from Member States "*to provide for adequate legal protection against any person 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 copies of works or other subject matter protected (...) from which electronic rights management information has been removed or altered without authority,

if such persons knows, or has reasonable grounds to know, that by so doing he is inducing, enabling or facilitating an infringement of any copyright or any rights related to copyright as provided by the lax, or of the sui generis right."

This text is very similar to the WIPO provision. It is worth mentioning that the definition of 'rights management information' covers the terms and conditions to use the works as well, which entails that the licence, that might be a mouse-click contract, or notice attached to the work are protected. In the case of an ERMS, it means that all digital information related to content and processed by the system can not be removed or altered without authority. It could be the digital identifiers, such as CIS or DOI, the Licence Contract or the conditions of each transactions.

This is not the case of the US Bill which restricts the definition of such information to the identification of the work and of the rightholder , unless the wording 'the information set forth on a notice of copyright' which appears in the US definition of copyright management information might be broadly construed as including the terms and conditions to use the work and the licence contract attached to the notice.

The recital 34 of the EU Proposal requires the compliance of such systems with the Data Protection Directive when such rights management information allow for tracing of on-line behaviour and consumption patterns by individuals. Such an assertion seems inaccurate given the definition of 'rights management information'. The subject matter of protection is defined as "*any information provided by rightholders which identifies the work or other subject matter, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject matter, and any numbers or codes that represent such information*". The information related to the consumption patterns collected from individuals is neither provided by the rightholders, but rather automatically collected by the technical system, nor an information about the terms and conditions of use. Actually, the technical features which enable such a tracing exceed the mere function of rights management information. They belong rather to the features of a technical protection measure. Of course, some measures might enshrine both functionalities, the identification and rights management by tracing the works usages. This is namely the case of an ERMS. Nevertheless, it appears somewhat confusing to mention here such a tracing and data collecting. The compliance with the data protection has to be ensured at the stage of the setting-up of technical measures and at the stage of the effective tracing. The Proposal should provide such compliance by both rights management information and technological measures, contrary to this recital 34 limited to rights management information.

Maybe this confusion results from the access-based definition given to the technical measures. Such a definition can not easily be understood as enabling a usage-tracing. Therefore, the prohibition of article 6 of the Proposal to be applied to technological measures might be considered as providing no protection to the data collected from end-users and tracing the usage of works they carried. Their removal by the end-user might not be protected as such , while the preparatory activities and the manufacture of devices enabling such a removal will be covered by the prohibition enacted in article 6 of the Proposed Directive. Of course, it is important that the end-user is not allowed to defeat the technological protection so as to remove or modify the flow of data enabling the making of its account and requesting a due payment. However, we have seen to what extent the vague wording of the protection could cover the act of circumvention itself, and thus the act of removal of such digital information. As a conclusion, we would recommend that the definition given to the technological measures should be rewritten so as to cover the systems or devices enabling to trace usage operations and hence to process personal data.

The forbidden activity, in order to benefit from protection, should lead, or be preparatory to, an infringement of an intellectual property right provided by law. This requirement could not be easy to work in practice.

The US Bill[105] adds to the prohibition of removal and alteration of copyright management information, the providing, distribution and importation of false information. Maybe in Europe, such activity might be covered by the criminal offence of forgery. It should be useful anyway to explicitly stress in the Proposed Copyright Directive that the provision of false information is also prohibited. Another difference is that the Bill restricts the requirement of the knowledge of the consequence of copyright infringement to the distribution or performance of works with an information having been removed or altered. The mere removal or alteration only requires an intention to be illicit.

Finally, the Bill prohibits that such information relates to the user of a copyrighted work. This prohibition can be understood as there is no Data Protection Regulation in the US, even if such a provision resumes the confusion appearing in the European text. This prohibition would prevent a proper functioning of ERMS which need to process user's personal data for invoicing and conditional access.

---

105 sec. 1202 Bill

CONCLUSION

Certainly, the present regulatory framework can only provide unsatisfactory solutions for protecting Electronic Right Management Systems against circumvention. An appropriate remedy against the manufacture and commercial distribution of circumvention devices does not exist in most countries. Yet, a proper legal protection of any technological measures or devices aiming at protecting and managing IPR in the Information Society would be a strong incitation for their development and their utilisation by rightholders. The protection envisaged in the WIPO Treaties and in the Proposed Directive on Copyright is to be welcomed.

Nevertheless, in some aspects, such a protection appears somewhat inappropriate, at least as far as ERMS are concerned. Firstly, as regards the Proposed Directive, the ERMS seems to be covered by the scope of application as envisaged for the rights management information while not being in all cases protected as a technological measure, namely where the system merely manages the rights without restricting the access to the copyrighted application. Moreover, the ERMS could be covered by the Proposed Directive on the protection of conditional access services. This threefold protection is largely different as regards their scope of application, the prohibited circumvention or defeat devices, the prohibited acts and the level of knowledge of a possible copyright infringement to be required.

Finally, the boundaries of the protection versus a legitimate exercise of copyright exceptions is only stressed in the Proposed Directive on Copyright, even if its consequence remains uncertain. This could entail that a exception defence could take place according to the enabling text. It would be easy for the ERMS to invoke rather the conditional access protection or rights management information protection which do not address the copyright exemptions, than the technological measures protection.

On the other hand, the rationale behind these protections is somewhat puzzling. Some of the consequences of the envisaged protection let think that what is actually protected is rather the investment devoted to the development of the technology.

This is why we would be inclined to the adoption of a consistent computer crime regulatory framework which would prohibit any manufacture and commercial exploitation of circumvention or hacking technology whatever its purpose, any unauthorised access to a remunerated services or any removal or modification of a technological information or identification attached to a digital content. As regards the act of circumvention carried out by

an individual, it should be prosecuted only upon strict requirements such as maliciousness.

Such a regulation should be horizontal and cover a large field of application, whether IPR content, on-line services, etc... This does not prevent the legislator from considering the specific problems that each technology raises in each particular field of law. This is true for instance for the balance of rights which could be threatened by a blind application of a protecting technology. Nevertheless, such attention should be made before dealing with the protection of the technology itself. Otherwise, there is a risk that either the protection would be fragile, either the exercise of the exceptions would impose a too heavy burden on the user.

II. DATA PROTECTION*

1. INTRODUCTION

For the purpose of determining the kind of personal data that is likely to be processed by an ERMS, various functions of ERMS could be distinguished according to the level of "sophistication" of the technology. The first-and most obvious function- is that of managing intellectual property rights. The underlying technology must therefore enable the developer to precisely track the kind of protected material that is being accessed, printed or copied, who is doing so, from what terminal, thus potentially enabling the promoter to assess the precise profile of a user, the right holder himself and eventually of the market. The second function- or level of sophistication-could integrate the transfer of EDI messages-or standardised contracts-between parties (originators, producers, providers, users,...) which will also lead to the processing of personal data[106]. The transfer of payments with the intervention of a banking organisation could be envisaged at a later stage.

The second distinction which is useful to draw conceptually when designing an ERMS is that of an "anonymous interface" from the privacy point of view which acts as a kind of filter that removes the personal data. Such would happen for example in a case where an on line provider receives from a user a nominative request for a copyrighted material who then transfers the request (which becomes anonymous) to a central data base. The central data base then sends the material to the provider who transfers it on to the final user. If such a scenario is followed, the central data base will not be processing any personal data relating to the user. He will on the other hand probably be processing personal data relating the rightholder himself.

In Cited terminology, the data subject could be one or other of the following agents: originator, publishers/producers, collective end-user[107], individual end-user or private end-

---

* Author : Michele LEDGER & Sophie LOUVEAUX

[106] The use of EDI does not strictly carry implications from the data protection point of view for the setting up of an ERMS, but the various EDI intermediaries (such as the service provider) do have to respect data protection regulations.

[107] In so far as a collective end-user such as a company could appoint a person who will be responsible for

user. Additionally, such data could be transferred in no time over the network to any other terminal, in any country of the world.

In legal terms, the developer of an ERMS will be *"processing personal data"* which is why account will have to be taken, when developing or deploying an ERMS, of the legislation on the protection of privacy.

In an effort of harmonising the legislation of the Member States, the Council and the Parliament have recently adopted Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and of the Free Movement of Such Data[108], referred to below as the directive[109].

The directive[110] provides that Member Sates shall have to bring into force their laws, regulations and administrative provisions necessary to comply with the directive at the latest by the end of a period of three years from the date of its adoption i.e. by the October 24, 1998, which is why account will be taken in this paper of the rules contained in this piece of legislation.

2. Scope of Application of the Directive

The rules contained in the directive shall apply whenever personal data is processed by any person whose activities are governed by Community law[111]and who is established on the territory of a Member State[112]. Article 4.1. (c) also specifies that a Member State shall apply the provision it adopts pursuant to the directive to the processing of personal data where use is made of equipment, automated or otherwise, situated on the territory of the said

---

obtaining the right to access and to make use of the copyright application.

108 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 23 November 1995, L281, 31).

109 Mention can also be made of Council of Europe convention n°108 for the protection of individuals with regard to the automatic processing of personal data. 28 january 1991.

110 Article 32 of the directive.

111 Recital 12 of the directive.

112 Article 4.1 (a) of the directive. Recital 19 specifies that the establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and that the legal form of such an establishement is not the determining factor.

Member State, thus indicating that the determining factor is not so much the localisation of the person that is responsible for the processing but the place where the methods of collection are situated.

2.1. Personal Data

The Directive defines personal data as meaning "any information relating to an identified or identifiable **natural person** ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[113]. Pursuant to the very broad definition, reference to a bank account number could therefore be considered as personal data.

On the other hand, the information must relate to a natural person. Consequently, information relating strictly to a legal entity such as a collective end-user, in Cited technology, should a priori not be considered as "personal" data. Nevertheless, the legal entity will in most cases appoint a physical person who will be in charge of putting in the requests and who will receive the personal keys to decrypt the material-which will mean that personal data will be collected.

2.2. Processing

For the purpose of the directive, "processing of personal data" shall mean "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

---

113 Article 2 (a) of the directive.

3. The Controller and the Processor

3.1. Who ?

Whenever personal data is processed, and application is therefore made of the rules contained in the directive, a controller will have to be appointed who shall be "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, ..."[114].

The controller should not necessarily be the person who actually processes the personal data. The controller is the person responsible for the determination of the purposes and means of the processing. The actual processing operations may be carried out by another person on behalf of the controller referred to as "the processor" in the directive "*who shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*"[115].

Since the controller is mainly responsible for respecting the principles laid down in the directive, identification of the controller -and of the processor - is therefore paramount when deploying an ERMS.

Recital 47 of the directive suggests that a telecommunications operator or an access provider shall not be considered as a controller with regard to information placed on the network by his clients, because they do not actually process the personal data contained in the network by their clients. Such would be the case however, when processing user-related data for the billing of the service.

The controller shall therefore be the person who can effectively exercise control -solely or jointly[116]- over the determination of the type of data that shall be processed, as well as the means and purposes of the processing.

---

114 Article 2 (d) of the directive.

115 Article 2(e) of the directive.

116 Important if ERMS are developed by a consortium of enterprises.

3.2. The Interconnection of ERMS

When an ERMS in one country -or continent- is linked to another ERMS located elsewhere, or when all ERMSs will become interconnected to one another, it will become important to determine the controller that will be responsible. A user located in Europe who wants a copy of a work by a Japanese artist will put in a request at a European ERMS who will transfer the request to its Japanese ERMS counterpart. The Japanese counterpart will search its own data base, download the material to the ERMS located in Europe who will send it on to the final user. In such a scenario, the European ERMS controller would be responsible for the processing of the personal data relating to the end user and the Japanese ERMS controller would be responsible for the processing of the data relating to the rightholder.

3.3.The Trusted Third Party Scenario

The question is now to determine in an ERMS scenario, with the intervention of a **"Trusted Third Party"**[117] (TTP), if the TTP could be considered as a controller or as a processor. If the TTP is able to exercise control over the determination of which type of data will be processed as well as the means and purposes of the processing, and if he is also willing to accept all the legal implications of carrying out such functions, a TTP could be considered as a controller.

Because a TTP will in most cases find it difficult to fulfil the above conditions, the TTP will probably be considered in most cases as a *processor* acting *on behalf* of the controller. Article 17 further specifies the conditions of appointment of a processor as well as the way in which the legal relationship between the controller and the processor is to be governed.

The controller must, where processing is carried out on his behalf, choose a processor that provides *a sufficient number and level of guarantees with respect to the technical security measures and organisational measures* governing the processing to be carried out and must ensure compliance with those measures[118].

The relationship between the processor and the controller must be governed by a contract or a legal act binding the processor to the controller and stipulating at least that the processor is to act only on instructions from the controller and the obligations relating to the security of the processing described below shall also apply to the processor.

---

117 A TTP could act as an "anonymous interface" see introduction above.

118 Article 17.2 of the directive.

3.4. The Controller's Obligations and Duties

a. General Liability

The controller is designated by the directive[119] as the central person who shall be primarily responsible for the obligations arising from the directive including those undertaken vis-à-vis the data subjects such as providing them with the adequate information, ensuring the effectivity of their right of access and of the remedies available to them (See below).

b. Security (article 17)

In order to comply with article 17 of the directive, Member States will have to impose upon the controller that he implements appropriate technical and organisational measures so as to protect the personal data against destruction, loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission over the network. Article 17 further specifies that having regard to the state of the art and the cost of their implementation, such measures shall have to ensure a level of security appropriate to the risks represented by the processing, and the nature of the data to be protected such as medical data for example.

c. Notification

The controller or his representative must notify the supervisory authority before carrying out any wholly or partly automatic processing operation. Such a notification must at least include:

-the name and address of the controller or of his representative;

-the purpose or purposes of the processing;

-a description of the category or categories of data subject and of the data or categories of

---

119 Article 23.1. of the directive.

data relating to them;

-the recipients or categories of recipients to whom the data might be disclosed;

-the proposed transfer of data to third countries (outside the European Union);

-a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken in order to ensure security of the processing[120].

4. What are the Principles that must be Respected ?

4.1. The Legitimate Purpose Principle

It is specified in article 6 of the directive that personal data must be processed fairly and lawfully. Fair processing means a most transparent processing as possible as concerns the data subject. Lawful processing implies the respect of the principles enacted in chapter II of the directive.

Article 6 also stipulates that the data must be collected for specified, explicit and legitimate purposes. One of the primary difficulties when applying the directive is to determine the purpose or the purposes of the processing. In order to determine the operations that fall under the heading of a processing, it is important to determine the purpose. The French "Commission Nationale d'Informatique et des Libertés" has defined an automatic processing as "a set of operations performed on a set of data with the view to achieve a determined primary function". This primary function, or purpose for using the data, is the purpose of the processing. This conception has the advantage of being technologically neutral. In an ERMS a number of purposes will probably have to be determined such as the following:

1) Vis-à-vis the users

-Invoicing;

120 Article 19 of the directive.

-client management

-Assessment of market profiles

-Payment

2) Vis-à-vis the right holders

-Rights management

-Assessment of market profiles

Furthermore grounds must be found in article 7 on which the processing can be based.

In the case of an ERMS, the criteria for processing personal data could be one of the following[121]:

The data subject has unambiguously given his consent; or

The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract. [122]

The first ground could be invoked in a scenario where a user accesses an on-line data base by providing his own personal data. In such a circumstance, it could be invoked that the data subject has unambiguously given his consent to the processing of his data that is necessary for the functioning of the data base. It must nevertheless always be kept in mind that the consent to the processing is specific[123] in the sense that it only relates to a particular use of the data for a specified-predefined purpose and that any modification of this purpose requires a new consent.

---

[121] See article 7 of the directive.

[122] Other grounds also exist such as when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data arre disclosed; or when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overriden by the interests of fundamental rights and freedoms of the data subject which require protection.

[123] See the definition of the data subject's consent in article 2.h of the directive : « any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed ».

The second ground is probably more relevant since there are many different types of contracts in an ERMS including electronic or paper contract[124] between the publishers/producers or distributors and end users. However, once more, only the data that is necessary for the performance of this contract may be processed. It will not be possible to further process the data for the purpose of doing a market survey as to how a work is being used if unambiguous consent was not given by the data subject and if the purpose was not specified and made explicit at the outset[125].

4.2. Data Quality

The directive lays down in Section I of Chapter II a number of requirements relating to data quality.

Personal data must also be adequate, relevant, and not excessive in relation to the purposes for which they were collected and processed, be accurate and kept up to date, and only kept for a certain period (i.e. for no longer than is necessary for the purposes for which the data were collected and processed[126]).

4.3. The Prohibition to Process Sensitive Data

Sensitive data which is data that reveal-even indirectly- racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life[127], is prohibited, unless the rules contained in article 8.2. are complied with.

---

[124] It is useful to note that for the purpose of keeping proof, article 17.4 specifies that the parts of the contract or the legal act relating to data protection ...shall be in writing *or* ***in another equivalent form***" thus suggesting possible equivalence between an electronic document and a written contract or legal act.

[125] Article 6.1.(b) of the directive.

[126] Article 6 of the directive.

[127] Article 8.1. of the directive;

5. The Rights of the Data Subject

The data subject has the right to be informed (4.1), the right of access (4.2.), the right to rectification (4.3.) and the right to object (4.4). The enforcement of these rights shall be guaranteed by the controller.

5.1. The Right to be Informed

When the data is collected from the data subject, the data subject has a right to be informed at the time of the collection at least of the following information:

-the identity of the controller or his representative;

-the purposes of the processing for which the processing are intended.

Additional information (such as recipients[128] or categories of recipients of the data, existence of the right of access and right of rectification) must also be provided if it is "necessary in the specific circumstances to ensure a fair processing in respect of the data subject"[129].

If, on the other hand, the data have not been obtained from the data subject himself, article11 provides that the data subject must be informed of the same elements and categories of data concerned described above at the *time* of recording or no later than at the time of disclosure to a third party (if such a disclosure is envisaged).

5.2. Right of Access

Pursuant to article 12, the data subject has the right to obtain from the controller or his representative without constraint at reasonable intervals and without excessive delay or expense confirmation as to whether or not data relating to him are being processed and information as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. He shall also have the

---

[128] According to article 2.g of the directive. "a recipient shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities may receive data in the framework of a particular inquiry shall not be regarded as recipients".

[129] Article 10 of the directive.

right to obtain communication in an intelligible form of the data undergoing processing and of any available information as to their source.

5.3. Right of Rectification

Article 12 (b) provides that the data subject has the right to obtain the rectification, erasure or blocking of any data, the processing of which does not comply with the terms of the directive, in particular because the data is incomplete or inaccurate.

5.4. Right to Object

The data subject is granted the right to object, at any time, on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, except if other wise provided by national legislation. This right to object to the processing is granted unconditionally on request and free of charge with regard to the processing for the purpose of direct marketing[130]. It is important to know therefore that a user could object-for no reason at all-to the processing of the personal data relating to him if the purpose of such a processing is to carry out direct marketing.

5.5. Right not to be subject to an automated individual decision

Article 15 of the directive lays grants the data subject with the right not to be subject to a decision which produces legal effects concerning him or which significantly affects him and which is based solely on an automated processing of data which is intended to evaluate certain personal aspects relating to him such as his performance at work, conduct, etc. Member States however will be able to provide exceptions to this principle notably when the decision is taken in the course of entering into or performance of a contract provided the request for the entering into or performance of the contract lodged by the data subject has been satisfied or that there are suitable measures to safeguard his legitimate interests.

130 Article 14 of the directive.

6. Transfer of Personal Data to Third Countries

The rule laid down in the directive[131] is that the transfer of personal data which are undergoing processing or that are intended to undergo processing to a country outside the European Union (third country) may take place only if the third country ensures an "adequate level of protection". Article 26 of the directive nevertheless provides that by the way of an exception, the processed data may be sent to a third country even though it does not ensure an adequate level of protection notably if, the data subject has given his consent or if the transfer is necessary for the performance of a contract between the data subject and the controller.

[131] Article 25 of the directive.

III. VALIDITY AND ENFORCEMENT OF ELECTRONIC CONTRACTS*

INTRODUCTION

Electronic Rights Management Systems imply the on-line conclusion of a number of transactions. They will be mainly between the distributor or the URM acting on behalf of the distributor and the end-users. Such contracts will be a licence encompassing the authorised utilisations of the copyrigthed application. Others could be between the originator and publisher and between the Publishers and/or originator and the distributor for upolading protected material in the application. In this case, rights and obligations of the parties may also be agreed upon before the setting-up of the application in a traditional and written. Anyway, all these contracts can be entered electronically and namely by a simple mouse-click. Therefore the validity of such an expression of the will to enter the contract has to be addressed.

Other main concern deals with the formal requirements of contracts for evidence value, for instance the written form required in the licence of copyright. This question is dealt with in the title IV of this deliverable.

1. NOTION OF THE CONTRACT

A contract can be defined as legally binding agreement upon which each party has certainly expressed his consent. Agreement arises as a result of offer and acceptance, but a number of other requirements must be satisfied.

In most European Countries, e.g. in France and Belgium, there are four key requisites for the existence and validity of a contract :

*consent of the parties : the parties must have an intention to create legal relations

*the parties must have capacity to contract

* Author : Séverine DUSOLLIER

*the contract must have a legal object

*the contract must have a legitimate cause

In an electronic environment such as the Internet, all these requirements are challenged. How can one determine whether the other party, at the other end of the Web, has the legal capacity to contract ? What is actually the object and cause of a contract sometimes entered between two machines ? It is particularly relevant that the object of the contract is sufficiently determined as well as the key elements thereof.

However, the main issue to be stressed is the consent of the parties. In contracts entered electronically, the consent is expressed in an electronic form by using a machine. In an open network such as the Internet, parties can carry out transactions by new methods. In all likelihood, a number of commercial transactions, particularly with consumers, will be entered by clicking on an icon such as 'I agree' or 'I accept'. The main question is whether so called mouse-click paramounts to an expressed will to contract. In general, no particular formality is required for the creation of a valid contract. It may be oral, written or even implied from conduct. Therefore the question is whether a mouse-click can be regarded as a conduct certainly implying a will to contract.

Another key issue is to identify where and when a contract is entered. This is the question of the contract between absent people, i.e. when parties are not physically in front of each other when concluding the contract. When the offer of a party is accepted by another to form a contract in a different place and at a different time than that where the offer was proposed, the time and the place of the formation of this agreement has to be determined.

2. WAYS OF CONTRACTING IN THE CITED REFERENCE MODEL

In the Cited Reference Model, it is foreseen that a contract occurs at each transaction carried out by the parties. Such a transaction consists of requesting the access to and use of a copyrighted application. Each time the object of a transaction, i.e. the requested content and usage right is agreed upon and a price is determined. Therefore, we should consider that each transaction paramount to a contract. The consequence thereof would be that any requirement we will stress further on should be met at each transaction. For instance, a clause should agree upon the use of electronic means to form the contract, a evidence agreement could be made, etc... . This could be pretty heavy and user-unfriendly.

Another contract could be agreed upon in the course of the ERMS operation. The first time a user logs into the system, the general terms and conditions of the ERMS operation can be displayed and an agreement can be concluded. We can understand this first step as being a general business agreement to rule the further transactions taking place between this now-identified user and the URM or distributor.

This first agreement should address the following points, at least as regards the validity of further transactions :

- the validity of the mouse-click process to bind te parties;

- the obligation of recording all electronic evidence relating to entered transactions;

- the acceptance of the parties as regards the validity of electronic transactions and the evidential value of electronic documents;

- the fact that the licence will be applied to all further transactions entered between the same parties.

At each transaction, the system should display, at least, the following minimal informations :

- the object (requested content and usage rights)

- the price

- a reminder of the fact that the licence agreed upon between the parties still applies to this transaction.

- the period of time during which the conditions and price remain valid.

3. Validity and enforceability of on-line contracting

3.1. Introduction

The issue of determining what the consent could be in an electronic environment has already been considered in the legal thinking surrounding the EDI. Of course the electronic contracting being envisaged by the Cited Model is not really a EDI which was primarily a method for carrying out business-to-business transactions in a closed electronic network. Nevertheless some principles developed in the EDI framework could be transposed to click-mouse contracting.

3.2. Rules developed in EDI

The legal thinking around the EDI has resulted in the adoption of the European Model EDI Agreement which sets up minimal rules to be agreed upon by the parties for the acceptance and validity of operations carried out by EDI. The main principle is thus the validity of the transactions exchanged by EDI where the parties have accepted such a way of contracting. According the article 9 of the Model EDI Agreement, "*the parties accept that transactions are validly formed by exchange of EDI messages, and expressly waive any rights to bring an action declaring the invalidity of a transaction concluded between themselves on the sole ground that the transaction took place by use of EDI.*" This agreement has to be entered in a written form priorily to the exchange of transactions by EDI.

The electronic contracting by EDI or in an open environment are similar, albeit being subject to major differences :

- the EDI normally takes place in a closed electronic network contrary to the click-mouse contract which will be primarily used in open networks. Therefore, the parties don't know each other, contrary to what usually happens in an EDI relationship.

- the EDI process is entirely automatized while the electronic contracting, namely by click mouse process is characterized by the presence of one partie behind his computer screen.

- the automation of EDI is not present in a click-mouse contracting where one party agrees upon the contract to be read on the computer.

- the EDI is mainly used between professional parties, while the electronic commerce requires a secure way of electronic contracting so as to validly bind consumers as well as

professionals .

• in the EDI, the parties often agree upon a prior declaration about the validity of the contract while in electronic commerce, users can enter a digital contract occasionally. The conclusion of a prior agreement dealing with the validity of the on-line contract might be entered in a written form prior to any on-line transaction, as in the EDI. Nevertheless it is not a suitable solution for electronic commerce where the transactions often need to be concluded rapidly for each envisaged transaction .

Beyond these differences some rules developed in EDI should be resumed for other forms of electronic contracting in open networks. For instance, an acknowledgement of receipt of message might be required (article 4 of the European Model EDI Agreement), a time limit for processing the message might be imposed (article 5), and whenever it is possible, the parties should beforehand enter interchange agreement (article 9). Whatsoever, the validity of electronic contracting should be linked to a proper level of security (article 6 of the European Model EDI Agreement) and to an obligation to keep records of the transactions entered (article 7). Therefore, the European Model EDI Agreement could be a good basis for drawing the main principles of electronic contracting.

3.3. Click-mouse contract

a. Analogy with shrink-wrap licences

A number of legal commentators[132] have underlined an analogy between the click-mouse contracts and shrink-wrap licences. A shrink-wrap licence is often used in the sale of computer software. This particular licence has been developed in the computer industry to fill the gap of direct contact between the software company (i.e. rightholder of the software) and the end-user so as to bind the user to terms and conditions to use the software often bought at a retailer. The licence to use the software can thus be seen through the shrinkwrap in which the software is packed. It is assumed that the user can read the licence through the shrinkwrap before opening it. If the end-user does not agree with the terms, he is able to

---

132 Institute for Information Law, "Formation and validity of on-line contracts", Imprimatur Report, Amsterdam, June 1998.

FARELL F., "From Shrinkwrap to Cyberspace. 1996, http://www.weblocator.com/attorney/briefs/ff2.html

GRIFFITHS D. "Contracting on the Internet", EIPR 1997, p. 4-7

LEMLEY M.A., "Shrinkwraps in cyberspace", Jurimetrics Journal of Law, Science and Tachnology, vol. 35 n°3, 1995, p. 311.

return the software to the retailer so as to be refund. Otherwise, since he opens the package, he is assumed to be bound by the terms and conditions enshrined in the licence.

Its validity has been recently recognised in the United States, the UK and the Netherlands.

In the United States, the recent decision ProCD v. Zeidenberg[133] has changed the former case law which held shrink-wrap licences unenforceable. The facts were the following : Zeidenberg had bought a CD-ROM containing an information database. The licence which was a shrinkwrap one, prohibited a further commercialisation of the data while providing that the user will be bound by the terms of the license as soon as he uses the CD-ROM. The first screen appearing when using the CD resumed the terms of the license. Zeidenberg made available the data on the Internet against this prohibition.

The producer of the CD-ROM sued Zeidenberg for breach of the contract. Zeidenberg argued that the licence was not enforceable because he was not aware of its content at the time of the sale.

The US Court of Appeal decided differently by stating that "*a contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract*". As a conclusion a shrinkwrap licence is enforceable within the limits of normal rules of contract law.

The UK case[134] was somewhat different since it was the user who argued for the validity of the shrink-wrap licence and not the software company. Adobe wanted to return for refund a software bought from the retailer Beta. Such a right of return was stated in the shrinkwrap licence accompanying the software. The retailer Beta refused such a return and eventually sued Adobe for payment of the software. The court has held valid the shrinkwrap licence and gave effect to the license towards Beta, which was a third party to this contract being actually entered between the user and software producer by virtue of a Scottish doctrine. However, the principle of the validity and enforceability of shrink-wrap license has been clearly established.

Whatsoever, this case law is very limited and no other countries have accepted the validity of shrinkwrap licence as such.

Furthermore, the analogy drawn between the shrink-wrap licenses and click-mouse contracts is somewhat defective. Indeed, the click-mouse contract might be considered as a further stage of shrinkwrap license where the user accepts the terms and conditions of access and use by clicking on an icon such as 'I agree ' or 'I accept'. As in shrinkwrap license, once

---

133 ProCD Inc. v. Zeidenberg 86 F. 3d 1447 (7th cir. 1996), LEXIS 14951

134 Beta v. Adobe (1996) F.S.R. 367, see GRIFITHS D., "Contracting on the Internet, EIPR 1997, n°13, p. 4

the user gets into the service or downloads the goods or information offered, he is deemed being bound by the terms and conditions priorily appearing on his computer screen. However, some differences should be highlighted :

- In an on-line contract, it is technically feasible to record precisely the click made by the user which ensures that the user has read the license or at least has been warned and is aware that his click paramount to an acceptance of the license.

- In an on-line contract, the user is aware of the terms of contract before downloading the goods offered. He can thus easily step back as no transaction has been legally entered at this stage. In shrinkwrap license, a sales contract has already taken place.

- In an on-line contract, normally the payment will be made after the access to the service and to the click accepting the contract. In such a case, if the user does not agree with the terms of license, he can easily not pursuing his on-line transaction. In a shrink-wrap license, since the price has been paid before being in a position to disagree with the terms and conditions of use, the return of the software is less easy to accomplish.

b. Validity of click-mouse contract

All these differences argue for a easier legal recognition of click-mouse contract. However, as far as we know, no case law has explicitly validated such on-line contracting at present.

The legal rules applicable to this sort of contract can be described as follows. In most cases, the formation of contract does not require the compliance with any particular formal conditions, except for evidence value or for certain contracts (e.g. insurance contracts, travel contracts in some countries, etc...). The only rule is that the consent of each parties have certainly met each other. The consent is ruled in most regulatory framework by the 'principe de l'autonomie de volonté ' or 'rule of the autonomy of will'[135]. This concept means that the parties are free to contract or not, to choose their contractant, to define the content of the contract and the way of expressing their will. Therefore, the parties should be free to decide to enter their contract on-line and by a process such as mouse-clicking.

We think that there is a major difference here with the EDI where two automatized applications enter transactions. In this case, the questions of what the human consent is and how it is expressed in EDI transactions were particularly relevant. In on-line contracting, the

135 ELIAS, Lieve, GERARD, Jacques, WANG, Gien Kuo, "Le droit des obligations face aux échanges de données informatisées : l'EDI, la formation des contrats et la responsabilité des opérateurs de réseau", Cahiers du CRID n°8, Story-Scientia, 1992

contract has been drafted by a human and placed on-line to appear on the computer screen of any user who want to access to services or goods. This user is present when he gives his consent to the contract. Therefore both the offer and the acceptance of the contract are human-driven.

The main issue concerns the multiple transactions entered at each time a registered user wants to get access to a work component. In this case, we have seen that the scope and the price of the license to use the work component are the object of the contract. The other part of the transaction is here entered by an 'electronic agent' which is a computer program, in the case of the Cited Reference Model. A specific interface initiates and responds to electronic messages without being reviewed by an individual.

However, in both cases, there is no legal certainty so as to whether the mouse-click carried out by the user will be accepted as a valid expression of will to contract by the courts. Therefore, it should be addressed by European or national legislators.

Meanwhile it should be paid attention to keep a due record of each transaction entered both in an electronic form and in a easily-readable form for the purpose of evidence.

3.4. Legal initiatives

a. The UNCITRAL Model Law on Electronic Commerce

The Model Law on Electronic Commerce is a non binding instrument adopted by the United Nations Commission on International Trade Law (UNCITRAL)[136]. Its purpose is both to state common principles with a view at inspiring national legislations on that point , and to enable parties to include or refer to its model clauses in their contract.

The scope of Model Law covers the use of electronic means for recording and communicating information. The Model Law applies to "*any kind of information in the form of a data message used in the context of commercial activities*" where 'data message' is defined as "*information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telgram, telex or telecopy*". Even if this definition does not explicitely cover an on-line transaction entered by a click-mouse process, it can result from the broad wording of data message. The Model Laws provides for some examples of concerned commercial activities

136 The Model Law is available on the UNCITRAL website : <http://www.un.or.at/uncitral>

as licensing, transactions for supply or exchange of goods and services.

Besides the legal recognition of admissibility and evidential weight of data messages, the legal equivalence of data message and writing form or hand-written signature, the Model Law deals with the formation and validity of electronic contract. By virtue of its article 11 § 1, it is said that "*an offer and the acceptance of an offer may be expressed by means of data message. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole gound that a data message was used for that purpose*".

The paragraph 2 provides that an enacting State can exclude the application of the first paragraph in certain instances to be specified. The objective of such a restriction is to enable the national laws to prescribe additional formalities, such as notarisation or some requirements for 'writings', for the formation of certain contracts[137]. This provision provides also that the parties are free to state otherwise. The principle of party autonomy is thus recognised.

Therefore nothing prevents the parties from including in their contract a clause similar to the article 11 § 1 of the Model Law validating the electronic form of the agreement. If the end-user is a consumer, it should however be paid attention that he explicitly agrees upon such a clause and therefore upon the validity of the electronic form of the contract.

b. The European Commission

The forthcoming directive[138] on electronic commerce might address the validity of electronic contracting, as it was announced in the Communication on electronic commerce. We do not know anyway whether this directive will be inspired by the UNCITRAL Model Law.

137Guide to Enactment of the UNICTRAL Model Law, 1996, n° 80, comment on article 11.

138This proposal for a directive has been announced for the end of 1998.

4. TIME AND PLACE OF THE FORMATION OF THE CONTRACT

A contract is formed at the time and place where the offer and acceptance met each other. This rule is easily applicable when both parties are at the same time at the same place, which was the common case in a physical world. In an on-line environment, the parties are inevitably in different places or countries when agreeing upon the contract. Since the transmission of the electronic data may take a certain time due to technical problems or to the necessary time to process the message, ascertaining the moment of the formation of the contract may also raise some problems.

The place where the contract is formed is relevant for the following reasons :

- it constitutes a important criteria to determine the competent jurisdiction and the applicable law; nevertheless, this consequence should not be exaggerated since the parties can choose the competent jurisdiction and the law applicable to their agreement.

whereas the time of formation has the following consequences :

- an offer is not rescindable as soon as the contract has been formed;
- the effects of the contract start since the formation of the contract;
- the legal capacity of the parties to contract has to be considered at the time of the contract formation
- the contract is ruled by the law into force at the time of the contract formation

The presence of a trusted third party in the Cited Model might complicate the determination of the time and place of formation of the contract.

Four different doctrines[139] exist in Europe to determine the time and place of formation of a contract so-called between 'absent people' :

---

[139] ELIAS, Lieve, GERARD, Jacques, WANG, Gien Kuo, op. cit.

1. *The theory of the emission* : by virtue of this theory, the contract is formed at the time and place where the acceptant has expressed his will to accept the offer. Thus, it is the point X1 mentioned in the figure below[140]. The relevant act would be where the user clicks on the icon to accept the offer. Therefore, the time could be registered by the system . On the contrary, the place would be more difficult to define. It could be the IP address of the computer by which the user has entered in the copyrighted application.

This theory applies in France[141].

2. T*he theory of the expedition* : the contract is formed at the time and place where the acceptant has transmitted his acceptation to the offerer. Here it is the point X2. In a click-mouse contract the difference with the first theory is pretty thin, since the expedition of the will to contract is implied by the click which is also the expression of this will.

This theory applies in the United Kingdom under the following exception : where the acceptation is made in a written form, the contract is formed when the letter has been posted ('the postal rule').

3. *The theory of the reception* : the contract is formed when the acceptation arrives at the domicile of the offerer, i.e. X3. This point should be in an ERMS application the computer system monitored by the URM or if the URM act on behalf of the distributor, the computer system of the former who is the offeror in the contract formation.

This theory applies in Netherlands[142] and in Germany[143].

4. *The theory of the information:* the contract is formed at the place and time where the offerer effectively takes knowledge of the acceptation, i.e. X4. The disadvantages of this solution is that this knowledge can only be taken by a human being and not by the automatized process which sustains the ERMS.

The Belgium has adopted a version of the information theory. Indeed the contract is

---

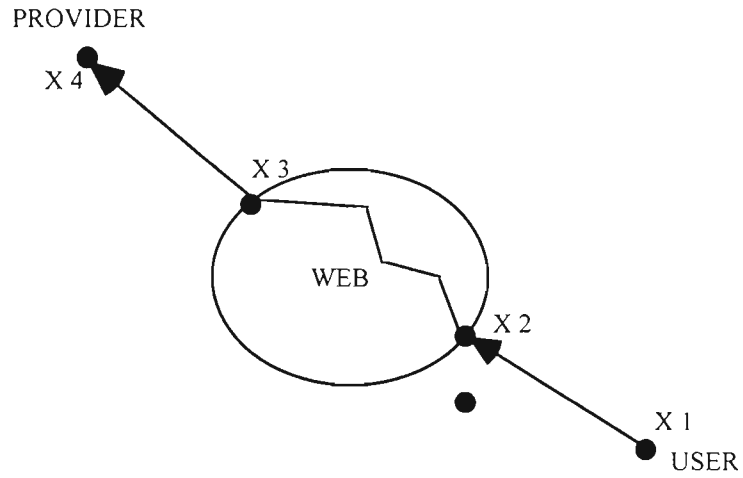
140 the figure is resumed from ELIAS, Lieve, GERARD, Jacques, WANG, Gien Kuo, ibidem

141 Cass. 07/01/1981.

142 art. 3.2.1. Nieuwe Burgerlijke Wetboek

143 art. 130 BGB

formed where and when the offeror has taken knowledge of the acceptance or would have reasonably been able to take knowledge thereof[144].



X 1 : The user expresses his will to accept the offer

X 2 : The user's will is sent to the provider

X 3 : The user's will arrives at provider's application

X 4 : The provider takes knowledge of the acceptation of his offer

The European Model EDI Agreement has stated that the contract "will be considered to be concluded at the time and place where the EDI message constituting the acceptance of offer is made available to the information system of the receiver"[145]. This is thus the theory of the

144Cass. 25/05/1990, J.T., P. 724

145 article 9.2.

reception. This solution is justified since the Model imposes to the parties to keep a complete and chronological record of all data messages, the so-called 'data log', which could be used so as to determine the time and place of the reception of the acceptance.

The UNCITRAL Model Law has not dealt with this point leaving the matter to national laws. But it defines what is the time and place of receipt of data messages, i.e. :

"(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs :

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee. "

whereas the time of dispatch is the place where the originator of this data message has its place of business.

We should be inclined to transpose the solution adopted in the EDI Model Agreement, i.e. the place and time where the reception of the acceptance takes place, while pro-viding that this time should be recorded by the data log ensured and operated by the URM.

5. Conclusion

Given the lack of a legal or jurisdictional validity of click-mouse contract, caution should be taken so as to enhance the security and evidence of the transaction. Moreover, the click-mouse contract should avoid terms and conditions which could be considered as excessive or surprising for the user. Such excessive terms could be the prohibition of the exercise of copyright exemptions, requirement of a pre-payment, limitation of liability and so on.

Finally the click-mouse contract should provide a clear information about the URM and distributor and some ways for the user, particularly when it is a consumer, to address his complaints. Therefore, the address and telephone of the ERMS operator or URM should

clearly appear on the Website. A e-mail address or a URL would not be sufficient in our view, even when dealing with business people.

Another practical advice is to draft short licences in such a way they can appear in their entirety on a webpage which could incite the user to read it.

We have also mentioned that the maintenance of an organised datalog of acceptance along with the terms agreed upon, should be useful for evidence purposes and for determining the time where a mouse-click has been made. The system should adopt digital signature and make authentication of documents reliable. It is also important that contract screens require unambiguous manifestations of assent or rejections.

IV. LEGAL ACCEPTANCE OF DIGITAL DOCUMENTS AND ELECTRONIC SIGNATURES . TRUSTED THIRD PARTY SERVICES*.

1. Introduction

The implementation and upgrade of the CITED model will lead to the possibility of entering "electronic" licence and usage contracts, chiefly between the distributor and the so-called end user. As explained below, some legal systems require licence contracts to be made in a written and signed[146] form . We shall analyse the purpose of the written requirement and attempt to see if an electronic document could be accepted or if an agreement could supersede the legal requirement of a written document. In order to carry out this analysis we will refer to the situation in national legislation regarding the way in which case law and legal commentators regard electronic contracts in general when national legislation requires a written document since, in many cases, there is no specific case law regarding electronic licence contracts because of their relative novelty.

We will then examine the evidential value of such electronic documents with a digital signature by considering the ability of telematic systems to achieve the same functions as obtained in an analogue scenario. The functions of the manual signature will be discussed in order to demonstrate that the digital signature fulfils the same function. The intervention of trusted third parties will be analysed in order to make operable the electronic signature (mainly with the support services functions) and in order to provide evidence (notarial functions).

---

* Author : Rosa JULIA BARCELO

146 In general, this requirement of a signature is addressed in the same way as the requirement for a written document. In other terms, if the Court does not admit as evidence electronic documents because only paper document are considered to fulfil the written document requirement, the Court, likewise, will not accept the digital signature.

2- Overview

2.1.- BELGIUM

The Belgian Act on Copyright and Related Rights of 30 June 1994 provides that economic rights can be transferred or assigned, in whole or part, according to the rules contained down in the Civil code. It is also said that *regarding the author*, all contracts must be evidenced in writing[147]. This requirement is therefore only valid regarding the author and does not concern licensees or assignees. It is obvious from this provision that the written requirement is provided "ad probationem".

There is no case law regarding this provision. Reference must therefore be made to article 1341 of the Civil code which lays down the general rule that a writing is required to evidence any legal act involving consideration in excess of 15000 B.F.

The Belgian case law and commentators to date have refused to acknowledge that a message stored in an electronic or magnetic document cannot be regarded as "written" with the meaning of this provision. Also, they have refused to accept a concept of signature differently than the hand-written one. Accordingly, the digital message will not be accepted as "private instrumentum" ex art. 1322 C.c., i.e., an instrument which is a written document accompanied by a hand-written signature.

Nevertheless, we should point out that the scope of the Civil Code could possibly be circumvented by application of article 1348 of that code, by pleading that the electronic message makes it impossible to evidence the matter in writing.

2.2.- FRANCE

Article L.131-2, al. 1 of the French CPI (L. 1957, art. 31, al 1) provides that representation, publishing and audio-visual production contracts as well as "free of charge authorisations of performance" must be evidenced in writing. Article 131-3 al.3 provides the same requirement in relation to audio-visual adaptation contracts. It is also certain that under French law, this requirement is "as probationem". It is interesting to note that article 131-3 al.2 provides that under special circumstances, the contract may be validly evidenced by exchange of telegrams. It also accepted that such a requirement is fulfilled by using telex or telefax technology[148] The law provides that in all other cases, reference must be made to

147 Article 3 of the Act.

148 See LUCAS, A. and LUCAS, H.J., *Traité de la propriété littéraire et artistique*, LITEC, Paris, p. 400 and

articles 1341 to 1348 of the Civil code.

Art. 1341 of the Civil Code prescribes the use of a written form of proof when any transaction involves a certain amount of money. Art. 1348 of Civil code eliminates the need to produce an original document under Art. 1341 when the conditions prescribed by Art. 1348 exist. In 1980 Art. 1348 was amended by Law L.n. 80-525, 12 July 1980), adding "material impossibility" (versus "moral" impossibility) to the conditions where an original document need not be produced. The courts and commentators have held that the use in transactions of electronic documents can make it materially impossible to produce a "written document" and hence excuses the need to produce such a document to evidence such a transaction.

2.3.- SPAIN

Article 45 of the Spanish Act 22/1987 of 11 November 1987 on intellectual property requires publishing contracts to be made in writing. Article 61 furthermore states that if such is not the case, the contract shall be null. From this latest article it could be inferred that the requirement of a written document is a condition of validity of the contract. In our view, this interpretation is contrary to the interpretation of article 1280 of the Civil code which requires contracts involved an amount exceeding 1500 pesetas to be entered into in a written form. Courts have interpreted this requirement as a mere "faculty" instead of being an obligation.

So long as electronic documents give proof of authentication and integrity, Courts have valued such documents in the same way as written documents[149].

2.4.UNITED KINGDOM

Section 90-(1) of the Copyright Designs and Patents Act of 1988 states that "Copyright is transmissible by assignment, by testamentary disposition or by operation of law, as personal or moveable property". Section 90 (3) specifies that "An assignment of copyright is not effective unless it is in writing signed by or on behalf of the assignor". By virtue of Section 90 (2) this provision is also applicable to licences, whether exclusive or non exclusive.

Written documents are generally construed in a wide manner under UK law as typing, printing, lithography and other methods of representing and reproducing works in a visible form.

In general two rules govern evidential issues in the United Kingdom: the best evidence

---

following.

149 STS 30-11-1981.

rule and the hearsay rule.

The "Best Evidence Rule"

Under UK law, a document will not be accepted in court unless it is an original document. Nevertheless it is not so much the signature requirement that constitutes the most important requirement in assessing the authenticity of the document (the signature does not have the same importance it has in civil law countries), as the elements that surround the conclusion of the document. Indeed, once the original document is produced, its author will have to attest its contents.

Conceptual problems have been raised concerning the application of the rule of producing the original document in relation to computer documents. In order for a copy to be admitted as evidence it is necessary that it be either signed (in which case it will be regarded as a original -"duplicate original") or that the party producing it evidences that it was impossible to produce an original document. In this last case, it will be sufficient to prove that the document was destroyed during the normal course of business or that it never existed. There is a controversy as to the question whether a document produced by a computer can be regarded as an original.

The "Hearsay Rule"

This rule is the second step in the admissibility of methods of evidence. The assertion of a fact, whether written or oral, is only valid in so far as it is put forward by a witness in court. This witness must have had a personal knowledge of the exposed fact. The hearsay rule is a consequence of the rule according to which the only methods of evidence that are admitted in court are those that the court can verify itself.

This rule also raised certain problems in so far as it could be applicable to computer documents. Concerning such documents the legislator introduced in 1968 certain provisions in the Civil Evidence Act by considering that such documents could be admitted in court provided the person who introduced the data had a personal knowledge of such data or else in the course of his functions received the data from a person who had the necessary knowledge.

Paragraph 2 of section 5 of the Civil Evidence Act determines the admissibility rules concerning computer produced documents. This act has now been replaced by the Civil Evidence Act of 1995 which has introduced a series of amendments in other Acts. Section 8 (1) of the civil Evidence act provides that "Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved-a) by the production of that document, or b)whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve".

2.5.- UNITED STATES

Section 204(a) of the 1976 Copyright Act provides that "a) transfer of copyright ownership, other than by operation of law, is not valid unless an instrument of conveyance or a note or memorandum of the transfer, is in writing and signed by the owner of the rights conveyed or such owners duly authorised agent". Non exclusive licences do not, however, have to be in writing under the terms the 1976 Act[150].

We are not aware of any case law concerning this provision, reference is therefore made to the Statute of Frauds. As matter of contract law, Uniform Commercial Code Art. 2-201(1) provides that generally "a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defence unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorised agent or broker." Generally the courts have held that electronic documents constitute "writings sufficient to indicate that a contract for sale has been made between the parties.[151]" As far as the signature requirement is concerned, U.S. law takes a similarly flexible approach. U.S. law views this question from the perspective of the purpose of the signature requirement, which is to authenticate the writing, that is to identify the document with the signer[152]. Although there is no case law on whether digital signatures fulfil the signature requirement of the statute of frauds, U.S. courts have held "signatures" on telexes to qualify, and, given their greater probity, it is likely that the courts will likewise accept digital signatures.

As far as the rules of evidence are concerned, neither the best evidence rule nor the hearsay rule have proved to be an impediment to the admissibility into evidence of electronic documents. The basic principle applied in determining whether a document should be admissible despite the hearsay rule is whether it is sufficiently *reliable*, and generally speaking electronic documents are regarded to be equally reliable and are admissible to the same extent as paper documents under the business records exception to the hearsay rule.

---

150 Section 101 expressly excludes "non exclusive licences" from its definition of "transfer of copyright ownership". See P. GOLDSTEIN. *Copyright*. Volume 1. p. 418.

151- BOSS, A. .*The legal status of Electronic Data Interchange in The United States*, . (Prepared as part of the Electronic Trade Document Project [ELTRADO] funded by the Volkswagen Foundation, 1992

152- KATZ, P.R.; SCHWARTZ, A. *Electronic Documents and Digital Signaturing: Changing the Way Business is conducted and Contracts are formed.* IPL Newsletter, Vol. 14, N° 2, 1996

3.- Agreement solution

Although, as we have seen, national laws of contract require most contracts to be in writing as a condition of evidence (or in order to be enforceable), it is generally permissible for parties to agree that contracts between them formed by electronic means are enforceable absent to any sort of paper document. Thus, for example, two parties could agree, in a signed paper document, that all future transactions between them in a particular context may be conducted by EDI, and that the electronic documents created in the course of EDI will satisfy the requirement of a "writing" under any applicable national law and will be valued in the same way. However, this may not be the case in all countries, especially in a consumer context or because it is a matter of public order[153].

4.-Value of an electronic document with digital signature

As we have seen above, in general the requirement of written document and a signature is addressed at the same time in national legislation. In other words, if the Court does not admit a electronic document as a written one because only paper documents are regarded to fulfil the written document requirement, the Court likewise will not accept the digital signature. That is the case for Belgium (1341 C.c.). Conversely, where the courts do accept electronic documents, they also will accept digital signatures. It would make no sense to admit an electronic document, and then to insist that it be accompanied by a manual signature. Of course, as in the case of manual signatures, once a court has admitted an electronic document accompanied by a digital signature, the court will evaluate the circumstances surrounding the digital signature to determine the evidentiary value it deserves. (See discussion below on trusted third parties, etc.).

In other words, the crux of the issue is to value correctly the electronic document with digital signature. For European courts to become more flexible about the admissibility of electronic documents and value of digital signatures, they must become more familiar with modern technology and begin to understand that electronic documents and digital signatures are at least as trustworthy as paper documents and manual signatures. In most cases, it should be possible for the courts to accept electronic documents and digital signatures by a teleological interpretation of existing statutes. In a few cases, for example where national

153 See HOEREN, T. *"The answer to the machine is in the machine: technical devices for copyright management in the digital era"*, Law, Computers & Artificial Intelligence", Vol. 4. n°2. 1995, p. 179 and references cited therein.

legislation explicitly require hand-written signatures, statutory amendments may be necessary to enter the modern age.

In view of this situation, Community action is justified. Because Member States do not consider electronic documents and digital signatures in the same way, this could prevent the Internal Market from operating correctly which could constitute a barrier to the development of technological innovation in this field. The Commission should in our view propose harmonising legislation on the evidential value of electronic documents and digital signatures.

4.1. Electronic Document

A written document, can be characterised as follows "Any way which reproduces the will of one (or more) person in a sufficiently durable form and in a way that can be read by means of an appropriate procedure is recognised." In evaluating whether an electronic document constitutes a written document, under this view, we must consider three issues: First, does the electronic document express a will? Second, can the electronic document be "read" in way that permits one to determine what it means? Third, does the electronic message exist in a durable medium?

Each question can be answered affirmatively. First, the electronic message expresses a will just like any other document. This is equally true of electronic messages made without immediate human intervention, because in such cases the message generated by a computer program without human intervention results from a decision made by a human being to write a program that will send a particular message under certain given circumstances. Second, even though the electronic message may be written in a binary electronic code, rather than a typical analogue printed language, it can be read using modern technology just as easily and reliably as a message written on a piece of paper in any traditional language. Finally, electronic documents are contained on magnetic media (such as diskettes, CD-ROMs, and hard disks) that are generally as reliable as traditional paper media.

Analytically, therefore, there is no reason not to include electronic documents within the scope of "written documents." However, let us now see what the civil law of various countries says on this topic.

4.2.- Digital Signature

a. Manual Signature

A signature is a sign of its originator's intent to be bound by something. Thus, a signature serves the following purposes:

1- It identifies the signer with the signed document (authentication of the origin of a message or document);

2- It ensures the signer's assent to the content of the message.

A paper signature identifies the signed matter less than perfectly: Experience shows how often signed documents are altered. Moreover, when trading partners do not know each other (which is frequent in international trade), the value of the signature is even lower. In light of these facts, we could maintain the acceptance of the manual signature is based on a sort of historical tradition rather than an effective ability to fulfil the purposes before mentioned.

Because, as described below, electronic signatures accomplish the requisite functions even better than manual ones, it would be consistent and appropriate to allow them to be used like traditional ones.

b-The digital signature[154]

For digital signatures based on asymmetric cryptosystem, two different "keys" are used, one for creating a digital signature by transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original, intelligible form.

The principle of public key cryptographic services acts as follows: each person is allocated his own *two* keys: The key used for creating the signed document is called the "*private key*," which is available only to the signer. The private key uses an algorithm dedicated solely to the holder of this particular private key to encrypt a message. Nobody else has access to this private key, and hence nobody else can encrypt a message in the same way. The holder of this private key is also allocated his own "*public key*," which when applied to messages encrypted by the holder's individual private key, will decrypt those messages -- and *only* those messages. (Thus, the public key will *not* decrypt the messages (i.e., recognise the digital signature) of any other person.

Because a particular public key can only decrypt messages encrypted using its holder's private key, and because the sender of a message is the only possessor of the private key, when somebody receives a message signed by the sender and successfully verifies it using the public key he is confident it belongs to the sender (see below), he can presume: first, the author of the message is the sender (authentication), and second, the content of the message received is the same as the one that was sent (integrity). The public key is "public" because it

154- BAUM, M., Federal Certification Authority liability and policy-Law and policy of certificate based public key and digital signatures, U.S., 1994.

is made available to the general public, for example through a national directory of public keys or through certificates issued by Trusted Third Parties (see below). Thus, one who receives a digital message can retrieve the relevant public key (i.e., the public key dedicated to verifying messages encrypted using the sender's private key) from the public directory and use it to verify the message.

In practice, digital signatures sign shorter "message digest" rather than the whole messages. In most public key techniques, a one-way hash function is used to produce a condensed version of the message, which is signed. Because the hashing method is a one way function, the message digest cannot be reversed to obtain the message, so the receiver also processes the received text with the hashing algorithm and compares the resulting message digest with the one the sender signed and sent along with the message. If the message was altered in any way during the transit, the digests will be different, thus revealing the alteration[155].

Summarising, the digital signature fulfils the same functions as the manual signature. Indeed, because with a well-structured and managed public and private key system, it is virtually impossible to tamper with a digital signature, the digital signature is actually far more reliable than the manual signature[156]. A system of commerce based on electronic documents and digital signatures thus will be a much more secure system than ever seen before.

The most popular algorithms for public key cryptosystems is the Rivest, Shamir, Adleman (RSA) encryption technique and DSS which has now been adopted by the national Institute of Standard Technology in 1994[157].

i) Trusted Third Parties

The trustworthiness of digital signatures, and thus the evidentiary value a court will give them, lies in the reliability of the keys: The keys must give satisfaction that the party with whom one is communicating is exactly the one who is believed to be (i.e., the key system

---

155- U.S. Congress, Ofice of Technology Assessment. Issue Update on Information Security and Privacy in Network Environments, Washington, D.C., 1995, P. 49.

156- Nevertheless, the ability of software to discover the private key from the public key is increasing as technology progresses. Accordingly, if the length of today's key is sufficient it may not be in the short future. Therefore, the necessary length of key to obtain a reliable digital signature should be under constant review.

Furthermore, technology must also ensure the security of the network. The management of the keys must occur in a secure environment.

157- National Institute of Standards and Technology, Federal Register/ Vol 59, Nº 96, 1994. Notices

must eliminate the possibility that an impostor will manage to secretly substitute his digital signature for the other contracting party by substituting his private key for the private key of another person). For an electronic contracting system to function properly, a contracting party must be confident not only that the messages sent were actually sent by the person they purport to have been sent by, he must also be able to demonstrate that his own messages were actually sent, for example to prove the acceptance of an offer to contract.

As far as authenticating the identity of a sender is concerned, this can be achieved *between trading partners* through bilateral agreements where the parties exchange encryption keys between themselves and provide the necessary technical set-up for their communication. (There can, of course, be no assurance that, for example, a rogue employee will not steal one's business partner's private key and send one encrypted messages using that key, but there is of course likewise no assurance in a paper environment that employees will not affix fraudulent signatures to corporate documents. The business risks and the legal question in both cases is the same: who bears the risk of loss in the case of fraud by third parties.)

But what about an open business environment?: How, for example in business transactions conducted between strangers on the Internet does one provide the requisite confidence that the person with whom one appears to be communicating is actually that person? The answer to this question is that such security can be achieved through the establishment of a legal regime creating independent "Trusted Third Parties" ("TTPs") who provide the requisite assurances of identity by binding public keys to the identity of their owners.

According to the standard X509, the activities of such TTPs fall into two categories. First, they provide so-called "*support services*" facilitating security of electronic transactions, including the creation, distribution and management of keys. Second, TTPs provide so-called "*notary services*" (offering proof of activities between the communicating parties)[158].

ii) Support services

Two systems can be stablished: certificate system and directory system. We will focus on the certificate system.

Under the certificate system, Party A goes to the TTP with his public and private keys in order to obtain a certificate that the TTP issues[159]. The certificate contains the following information: among others, Party A's public key, the identity of the owner, the cryptographic algorithms, the serial number, the identity of the Certification authority. Then, this information is signed by the Certification authority with his private key and the signature is

158- TEDIS- *Security in Open Environments*, July, 1994, Brussels

159- It is also possible to set up a system where the TTP generates the key pair.

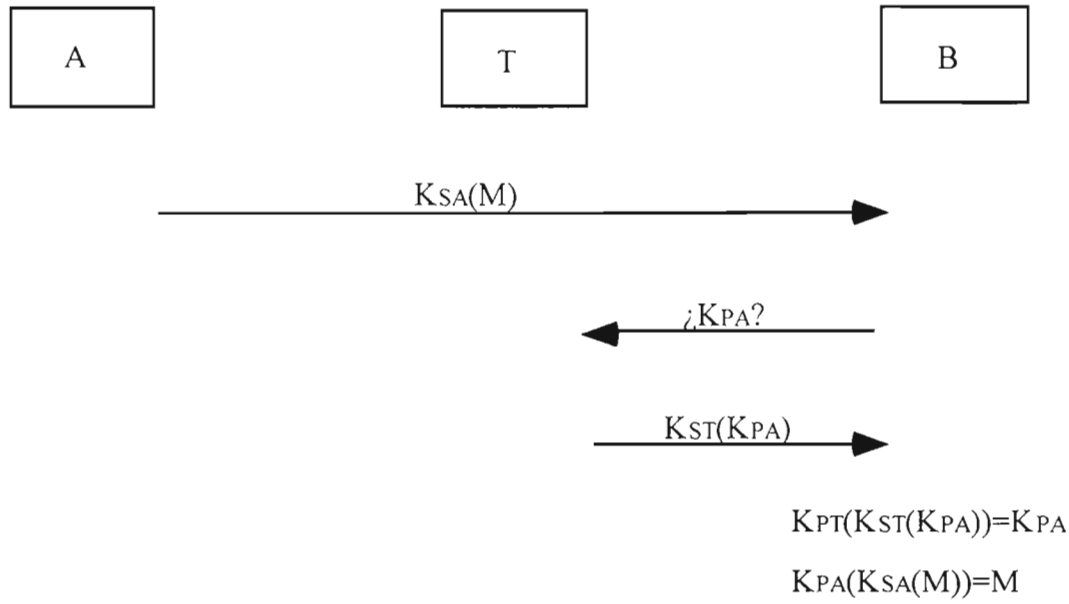
attached to the information not encrypted in order to form the certificate. Therefore, the certificate has two parts: the information non encrypted (to which the hash function has not been applied) and the digital signature itself.

When Party A enters into a transaction with Party B by sending Party B a message signed by Party A, also sends along with the message the TTP-issued certificate.

This will enable Party B to assure himself that the sender is actually Party A. He does so as follows: Because the certificate contains Party A's public key, signed by the TTP, and because the TTP's public key will always be publicly available, Party B can use the TTP's public key to verify the certificate sent along with the message by Party A and which contains Party A's public key. To do this, the hash function used by the Certification Authority (C.A.) to compute the digital signature is applied to the not encrypted portion of the certificate. The public key of the Certification Authority is then applied to the signature and the result compared with it. Both result must be identical.

Also, in certain systems, the receiving party does not trust the Certification Authority that has issued the certificate (mainly because in open systems he might not know the C.A.). Accordingly, if this Certification Authority has a certificate issued by another Certification Authority which the receiving party trusts, he can verify this second certificate. The process can be extended to the verification of a chain of certificates when there are more than two Certification Authority implicated.

It is important that the public key infrastructure sets up a certificate revocation list. This is a list containing statements that the links asserted by a Certification Authority between names and public keys are no longer valid (because the certifications have been revoked).



KSA(M) --> message signed with A's private key

¿KPA? --> request to obtain A's public key

KST(KPA)--> A's public keysibned by with T's private key

KPT(KST(KPA)) --> verification of A's public key with T's public key

KPA(KSA(M)) --> verification of the signed message with A's public key.

This system could also be carried out with a directory system. The directory contains a certificate of the public keys. The recipient of a message simply accesses to the TTP's certification directory.

iii) Responsibility of the certification authority:

It is hard to speak about the responsibility of the trusted third parties when there is not yet a widely accepted and consistent legal infrastructure with predictable principles governing the various relationships in a system of certificate-based public key cryptography.

In light of the roles to be carried out by the certification authority, mainly, certification[160] and keeping a record list with certificates, a legal infrastructure should allocate responsibility among the Certification authority and the parties issuing and relying upon a digital signature in the event the certification authority fails to bind a public key to the right owner or in the event a user compromises its private key[161].

It has been pointed out that could be applicable article 15, subsection 1, litra b) of the EC Product Liability Directive (85/374/EEC), that states that the producer of a defective product is not liable under the strict product liability regime, if he can prove that the state of scientific and technical knowledge at the time he put the product into circulation was not such to enable the defect to be discovered. Although the Directive may not apply directly to encryption services, the principle set forth in article 15, subsection 1, litra b) may be applicable. Indeed, most member states have decided to implement the development risk exception, even through that part of the Directive is not mandatory[162].

Financial responsibility may be assured through security arrangements such as surety bonds or standby letters of credit, or perhaps through liability insurance, when it becomes available.

iv) Who can play the role of TTPs?

The main requirement for a TTP, specifically for a Certification Authority is to be impartial and independent in order to inspire enough trust, first to the users, finally to the court which has to value the electronic document signed with a digital signature. So, users should be able to feel confident about the accuracy of the data.

So far, national banks and international chambers of commerce have demonstrated their interest to offer such services (e.g. in Belgium there is a TTP known as "System Isabel" provided by the Isaserver company).

Although from a technical point of view these entities (private and public) can provide the security services before-mentioned, the two following reasons indicate that a regulation of

---

160- Because of the legal nature of this document Naming and Certification roles have been treated together.

161- AMERICAN BAR ASSOCIATION, *Digital Signature Guidelines*, DRAFT, October 5, 1995

162- BRYDE ANDERSEN, M., *The Danish Teletrust- Initiative*, The EDI Law Review, Volume 1, N° 1, 1994

the legal framework of trusted third parties would be desirable:

a) An organisation offering security services under legal requirements would offer more reliability than others without any state regulation[163].

Fulfilling the legal requirements would allow a company/person to obtain a licence as a certification authority to offer security services. In our view, licensing establishes a minimal regulatory system to provide a level of reliability in certification authority practices.

Moreover, the licensed authority should be subject to control and audit regularly and the results of such controls will authorise the entity to continue its activity or will disauthorise it.

In short, for a court to grant value to the documents signed digitally the accuracy of the certificate is important . Thus, if the certificate has been issued by a entity subject to state control, it would be entitled to a presumption of veracity. The same is true for a user.

b) A legal infrastructure with predictable principles governing the various relationships would provide clarity: the duties and responsibilities of the certification authorise would become defined and this would favour the use of the technology.

Using national legal structures and not international ones would comply with the principle of subsidiarity and legitimate responsibilities of the Member States in the field of national security and public order.

vi) Notarial services.

As we have seen, an electronic signature identifies the author, and proves that the text signed and sent is the same text the recipient received (proof function). But a complete "proof function" requires the ability of the sender to demonstrate he sent the message and that is has reached the recipient in cases where he denies having received it. Here, TTP's can provide the necessary proof[164]. This role of the TTP would be very similar to the traditional notarial function (witness, authenticate or attest to the performance of certain actions by another party).

In any event, it remains a question of choice when to use the TTP and when not to, according to a specific electronic document. This value will depend on the reliability of Trusted Third Parties in carrying out their certification functions. This reliability would be enhanced by the establishment of a clear legal structure defining the manner in which TTPs

---

163- A Certification Authority without legal control (e.g., for economical reasons) might form an alliance with somebody to whom certifies a key and to act as another person (e.g., contracting as another person).

164- ALCOVER, G.; HUGUET, L., *Seguridad en la transmisión electrónica Válidez Jurídica*, Encuentros sobre Informática y Derecho, 1992-1993, Madrid

are to fulfil their certification functions.

5.- Conclusion

Electronic Copyright management Systems will lead to the conclusion of numerous types of contract. Such contracts could either be between the copyright owner and the producer (or publisher), the producer (or publisher) and the distributor (or on line service provider), and the distributor (or the on line service provider) and the end user. These contracts will involve the licensing or assignment of intellectual property rights. Reference will therefore have to be made to national copyright legislation which as we have seen usually requires that the contracts are entered into in writing. However, we have also seen that such a requirement sometimes only applies in relation to licence or assignment contracts entered into between the original copyright owner and the assignee or licensee (Belgium) or in relation to certain types of copyright licence contracts (France). In the case where the written requirement is not applicable because of national copyright legislation, reference will also have to be made to general contract law which could also require a written document.

From the comparative analysis carried out above, it can be said that generally, the requirement of a written contract is considered as a condition of enforceability or evidence and not as a condition of validity, which quite often will not preclude electronic documents from being considered as written documents because case law has sometimes adopted a flexible interpretation of the concept of written documents and because it is sometimes possible to enter a derogatory agreement.

The main issue is therefore to consider how the courts will value the electronic document. This will depend in our view on the use of the correct technology ensuring the same or -enhanced- values (authentication and integrity) as written documents which is the use of digital signatures with the intervention of trusted third parties. Furthermore, Courts must develop a flexible approach towards the concept of signature and written documents so as so include electronic documents and digital signatures.

In order to ensure legal certainty concerning the acceptance and value of electronic documents as evidence, a Community-wide harmonisation could prove necessary. Legislation must also be developed concerning the establishment and functions of trusted third parties.

V. CONSUMER PROTECTION*

Most of the contracts envisaged by the implementation of an ERMS consist of the on-line licensing and/or distribution of protected materials.

We will see that such contracts are distant-selling contracts covered by the EC Directive of 20 May 1997 on the protection of consumers in respect of distance contracts.

As a consequence, a number of obligations will have to be complied with when contemplating the setting up a service such as an ERMS that will lead to the conclusion of such contract.

We will therefore examine the relevant obligations on an ERMS context at the light of the EC Directive in question.

1) Field of application of the Directive

The Directive applies to "distance contract" which means any contract concerning goods and services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded.[165]

This definition which determines the range of application of the text, is in itself restrictive: it applies solely to contracts entered exclusively at a distance and the actual conclusion of the contract must take place at a distance.

The "means of distance communication" are defined as any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the

---

* Author : Jean-Christophe LARDINOIS

[165] Article 2 §1 of the Directive

conclusion of a contract between those parties.[166]

Such techniques as videotext, e-mail, fax and television are notably targeted. Information Society Services and contracting via the Internet are not explicitly covered by the Directive but its definition of the 'means of distance communication' has been broadly construed to include such new technologies.

The operator of a means of communication is any public or private natural or legal person whose trade, business or profession involves making one or more means of distance communication available to suppliers.[167]

Under this heading fall particularly : server centres, access providers and the operators of telephone and postal services.

The consumer is defined as any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession.

The supplier is seen as any natural or legal person who, in contracts covered by this Directive, is acting in his commercial or professional capacity.

2) Particularities of distance contracts

This Directive imposed certain obligations to the suppliers and envisages that the consumer should benefit prior information before the contract is concluded, that a confirmation of this information should be sent to him and he should be entitled to a right of withdrawal of 7 working days during which he may revoke the contract.

If the user ordering a intellectual work from a distributor is a consumer, the Directive on Distance contracts is applicable which means that the distributor will be obliged to provide the consumer the information prescribed by this Directive before entering the contract.

---

[166] Article 2 §4 of the Directive

[167] Article 2 §5 of the Directive

a) Prior information (article 4)

In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information :

- the identity of the supplier and, in the case of contracts requiring payment in advance, his address;

- the main characteristics of the goods or services;

- the price of the goods or services including taxes

- delivery costs, where appropriate

- the arrangements for payment, delivery or performance

- the existence of a right of withdrawal

- the cost of using the means of distance communications if this is calculated on another basis than that of basic one

- the period for which the offer or the price remains valid.

b) Confirmation of information (article 5)

These information will have to be confirmed either in writing or in another durable medium *"in good time during the performance of the contract and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him"*. We might say that the principle of a durable medium is of particular relevance to on-line distribution of goods and services in so far as we cannot expect a virtual distributor to provide the consumer with a confirmation on paper.

Therefore, the Directive allows that confirmation can be valid via medium like e-mail or floppy disc.

At this stage, it is worth mentioning that, according to the Directive's requirement, the consumer must "receive" these informations.

Thus, it can be argued that confirmation has not been satisfactorily validated if the distributor simply contents himself with posting it on-screen and leaving the consumer the obligation of downloading or printing out the information.[168]

In any event, the contents of the confirmation must take up the elements of the prior information and must indicate the existence or absence of a right of withdrawal, the supplier's address, the after-sales services, guarantees and the conditions for cancelling the contract where it is of unspecified duration or a duration exceding one year.

Finally, an exception to confirmation is foreseen by the Directive for those services which are performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication. This would not be normally the case in an ERMS where the service will be invoiced by the URM or the distributor.

c) Right of withdrawal (article 6)

The Directive provides a right of withdrawal in favour of the consumer who has a period of at last seven working days in wich to withdraw from the contract without penalty and without giving any reason.

While the Directive clarifies the starting date for this period by distinguishing between goods and services, this document does not define the notion of goods and services.

This is particularly relevant considering the moment of commencement of the period during which a consumer has the right to withdraw from a contract concluded at distance.

In fact, for goods, the period starts from the day of their receipt by the consumer and for services, it starts from the day the contract was concluded or from the day confirmation was received - in the event that this took place after the contract was concluded - on the condition that this delay does not exceed three months since the Directive envisages a further respite of three months applicable in those cases where confirmation has not taken place.

A problem of qualification of an on-line contract between a producer and a consumer may be decisive at this level.

On a European Commission position, it seems that such a contract has to be qualified as a service contract rather than a contract dealing with goods .

---

168 Anne SALAUN, "Electronic commerce and consumer protection" in les cahiers du juriste ...

The term of the right of withdrawal will run therefore from the date of conclusion of the contract considering well that if confirmation takes place within this term of three months, the seven days notice starts to run from the date of reception of confirmation [169].

Exercising the right of withdrawal obliges the supplier to reimburse the sums paid by the consumer. [170]

Article 6.3. of the Directive states some contracts for which the consumer is not allowed to exercise the right of withdrawal.

One exception concerns the provision of services if performance has begun with the consumer's agreement, before the end of the seven working day period

This exception could be of application in an ERMS system and more generally, in on-line services which are downloaded such as program, ... whose nature does not allow restitution.

Nevertheless, the ERMS system could provide such a right of withdrawal in its contract after having offered to the user a "sample" so as he can check the compatibility of the offered content with his own system. In this case, the right of withdrawal could be justified.

Finally, one criticism could be made one this point : how is the consumer informed of the lack of a right of withdrawal for this kind of service since the Directive does not envisages such information until the confirmation stage ?

Another exception to the right of withdrawal concerns contracts "for the supply of audio or video recordings or computer software which were unsealed by the consumer".

In an ERMS environment, one could argue that a copyrighted work could be digitally "unsealed" by mouse-clicking.

This exception would therefore apply on that matter.

As a conclusion, we suppose that the right of withdrawal should not be applicable in the case of on-line delivering of copyrighted content.

---

169 Article 6, last §

170 Article 6 §2

d) Contract performance (article 7)

The supplier is obliged to execute the order within a maximum of 30 days from the day following that on the consumer forwarded his order to the supplier.

The parties are nevertheless free to contract another term of execution.

e) Payment by card (article 8)

The Directive has thought to resolve the potential conflict between anticipated payment (implicitly authorised in the Directive) and possible withdrawal by the consumer in foreseeing an article 8 :

The Directive leaves Member States the care to ensure that appropriate measures exist to allow a consumer to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts and in the event of fraudulent use, to be recredited with the sums paid or have them returned.

3) Special protection

a) Inertia selling (article 9)

Consumers are protected against certain aggressive sales method : the Member states have to take the measures necessary to prohibit the supply of goods or services to a consumer without them being ordered by the consumer, beforehand, where such supply involves a demand for payment and exonerates the consumer from all payment in the event of unsolicited delivery

b) Opt-in and Opt-out (article 10)

The consumer's prior consent is required for any commercial communication issuing from automated calling systems without human intervention, or from fax machine (Opt-in technique).

On the reverse of this, the Opt-out technique, the consumer must take steps to oppose messages using other forms of telecommunications.

VI. LEGAL ISSUES OF ELECTRONIC PAYMENTS*

1. Introduction.

The legal answers given to the questions related to the payment of a service provided by an ERMS (Electronic Rights Management System) strongly depends on the kinds of payment chosen.

The person or the company which manage the database and sells the access to the copyrighted application has different possibilities, which depend on the kind of client and on the international or national character of the payment.

1.1. The pre-payment of a subscription:

If the customer is a professional (e.g. a company or a university) the best solution would be the pre-payment of a subscription whose balance of the amount would be reduced after each use.

This subscription can be paid online with an electronic funds transfer instrument (credit or debit cards, electronic wallet..) or off-line with a funds transfer.

If both, the merchant and the customer are living in the same country, the merchant should pay attention to terms of the contracts between the issuer and the holder of the electronic fund transfer instrument and between the issuer and himself. The most important articles of the contracts are those related to the liability and the possibility sometimes offered to the holder to make a chargeback.

The most interesting text in that case is the European recommendation of 30 July

* Author : Laetita ROLIN

1997[171]*, concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (see part I).*

If the merchant and the customer are living in different countries, inside of the European Union, the relevant text to use would be the European recommendation on electronic payment instruments and in particular the relationship between issuer and holder (see part I) but also, the Directive 95/5/EC of the European Parliament and the Council of 27 January 1997[172] *on cross-border credit transfers (see part II) even if the payment is made by card.*

1.2 : The payment per use.

Another possibility is the payment per use of the copyrighted application, the disadvantage of this solution is that the amount of the payment will be very small, and if the system of payment is not adapted to micro-payment the fees and charges might make the payment really expensive. Moreover, if the transaction is international.

The adapted system should be a micro-payment oriented, online system. In that case, the relevant text will be the Commission recommendation on electronic payment instruments and (see part I) and if the payment has an international character, the Directive 95/5/EC of the European Parliament and the Council of 27 January 1997 on cross-border credit transfers can be used also to define the obligations, rights and liability of both the client and the banker.

But if an adapted system does not exist, the merchant should allow only the system of subscription.

---

171 Commission Recommendation 97/489/EC concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, OJ N°L 208, 02/08/1997 p. 0052. (hereafter the recommendation on electronic payments).

172 Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers, OJ L42, 14/02/1997, p.25.

2. The Commission on transactions by electronic payment instruments

2.1. Characteristics of the recommendation

a. Legal value.

From a national point of view, the Member States[173] generally use the technique of contracts to regulate the use of payment instruments like debit, credit, and chip cards.

But it seems that these solutions do not provide adequate answers. It is why the Commission issued a recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder[174].

A recommendation is not an obligatory Act for the member States. The content of the recommendation should not be implemented as such in the national laws. Nevertheless, the recommendation express a common view of the Commission and could be the basis of legislative action of the Member State.

Furthermore, the recommendation provides in article 11 that : " the member States are invited to take the measures necessary to ensure that the issuers of electronic payment instruments conduct their activities in accordance with articles 1 to 9 not later than 31 December 1998". Which means that the Commission intends certainly to take the relevant measures to put these rules into force in a way or another.

It is why this text can be considered as a good summary of what will be the legal framework in the field of electronic payments.

b. The scope.

The recommendation does not precisely concern the relationships between the merchant

---

173 And particulary France, Belgium, Luxemburg.

174 (97/489/EC), OJ L208, 02/08/97, p. 0052

and the consumer, but those between the issuer and the holder of the electronic payment instrument. However, the recommendation provides in article 5 (d) that the holder may not "countermand an order which he/she has given, except if the amount was not determined when the order was given". The issuer is supposed to execute the payment in all case. The problems arising in the relationship between the merchant and the consumer is not supposed to interfere in the payment process.

Furthermore, this solution is already provided in model contracts such as the contract concerning the holder of the card elaborated by the Groupement des Cartes Bancaires in France (free translation) :

"The issuer stays ahead from all disputes arising, i.e. other than those related to the payment, between the holder of the card and the merchant. The dispute can never be the base of the cardholder's (or of the accountholder), refusal to honour the payment by card"[175].

Even if it does not regulate the relationship between the merchant and the consumer, the recommendation is interesting because it allows the merchant to know exactly the burden of the risk he is carrying. Because, the recommendation imposes obligations and liabilities to both parties (the issuer of the electronic payment instrument and the holder). The merchant is not concerned by these rules but support the consequences, for example in the case of loss or theft of the electronic payment instrument. In that case, the recommendation organises a specific system of liability based on the obligation for the holder to notify the loss of theft to the issuer as soon as possible (see below).

3.2. Analysis of the recommendation

The principles developed are the following. This recommendation applies to the transfers of funds other than those ordered and executed by financial institutions, effected by means of an electronic payment instrument[176]. Such an '*electronic payment instrument*'[177] covers both remote access payment instruments and electronic money instruments in the sense that 'remote access payment instruments' means an instrument enabling the holder to access funds held on his/her account at an institution whereby payment is allowed to be made to a payee and usually requiring a personal identification number and/or any other similar proof of identity. This includes in particular payment cards (whether credit, debit, deferred debit or

---

175 article 6 8° "l'émetteur reste étranger à tout différend commercial, c'est-à-dire autre que relatif à l'opération de paiement, pouvant survenir entre le titulaire de la carte et le commerçant. L'existence d'un tel différend ne peut en aucun cas justifier le refus du titulaire de la carte ou du compte auquel elle s'applique, d'honorer le règlement par carte"

176 Article 1.

177 Article 2a.

charge cards) and phone –and home- banking applications.

On the other hand '*electronic money instrument*'[178] means a reloadable payment instrument whether a stored-value card or a computer memory, on which values are stored electronically, enabling its holder to effect transfers of funds. The recommendation applies in its entirety only if the instrument is reloadable, if it is not, only a few dispositions apply.

A last important definition is that of the '*issuer*'[179] who can be defined as "a person who, in the course of his business, makes available to another person a payment instrument pursuant to a contract concluded with him/her". This definition is broad enough to include the merchant in its field. Therefore, if in certain cases, the merchant and the issuer are the same person, the recommendation would be of a greater interest.

In the ERMS Business Model[180], it is said that the payment will be made either before a usage operation or a set of usage operations is performed, either after a usage operation. In the first case, it corresponds to the payment of a use right credit, in the second it corresponds to the payment of a use right charge.

At first blush, nothing entails that the ERMS operator could be considered as a issuer of electronic payment instrument. In most cases the ERMS will interoperate with a external electronic payment system such as a credit card, a cheque, a bank transfer, a chip card as Proton, etc...

In such case, the URM will be a merchant as regards with the electronic payment transaction.

Nevertheless, it is worth mentioning that the position of the merchant is and will not necessarily be that provided by the recommendation. The financial institutions such as credit card companies or banks impose on the merchant a standard agreement which contains a number of adverse provisions. For instance, the merchant is often liable if he does not respect the different security requirements[181] laid in the contract such has the obligation to verify that the card is not in opposition, that it is signed etc.

Yet, there is a case where the ERMS operator might be considered as an issuer of electronic payment instrument. Indeed, given the broad definition of the electronic money, it could be construed that if the end-user has subscribed to the IPR application protected by the

---

178 article 2c.

179 article 2e.

180 ECMS Model- Vol I : Business Requirements. Deliverable 2.2.2.. p. 36

181 See for example the model contract for the merchant written by the Groupement des Cartes Bancaires in France

ERMS for a long duration, the credit granted and managed by the system paramounts to a electronic money. Nevertheless, we do not think that even in this case, the credit charge operated by the ERMS can be regarded as electronic money. It is rather an automatic withdrawal of funds linked with a mandate given to the URM to pay himself at each transaction with this stored money.

Anyway, should further ERMS systems create their own payment instruments in the form of electronic tokens, this digital cash will be regarded as electronic money instrument.

Therefore, when the recommendation will be passed as a law in some countries, the ERMS operation should comply with its content.

a-Obligations of the issuer :

The obligations of the issuer create limits to the liability of the other parties such as the merchant and the holder.

This recommendation provides for an obligation to inform[182] the holder about the terms and conditions governing the issuing and use of electronic payment instrument. Such information must be made:

-upon signature of the contract or in any event in good time prior delivering the instrument.

-in writing including, where appropriate, by electronic means, in easily understandable words and in readily comprehensive form.

-at least in the official language or languages of the Member State where the payment instrument is offered.

Information obligation[183].

The terms include at least :

- the determination of the law applicable to the contract;

- a description of the electronic payment instrument, including where

182 article 3.

183 Article 3.

appropriate, the technical requirements with respect to the holder's communication equipment authorised for use, and the way in which it can be used, including the financial limits applied if any.

- a description of the holder's and issuer's respective obligations and liabilities;

- where applicable, the normal period within which the holder's account will be debited or credited, including the value date, or, where the holder has no account with the issuer, the normal period within which he/she will be invoiced.

- the types of any charges payable by the holder.

- the period of time during which a given transaction can be contested by the holder and an indication of the redress and complaints procedures available to the holder and the method of gaining access to them.

If the electronic payment instrument is used for a transaction abroad (outside the country of issuing/affiliation), the holder must be informed of the amount of any charges and fees levied for foreign currency transactions, including the relevant date for determining such a rate.

Subsequently to a transaction[184], the issuer supplies the holder with information relating to the transaction effected by means of an electronic payment instrument. This information, set out in writing, including where appropriate by electronic means, and in readily comprehensible form, includes at least :

(a) a reference enabling the holder to identify the transaction, including where appropriate, the information relating to the acceptor at/with which the transaction took place;

(b) the amount of the transaction debited to the holder in billing currency and, where applicable, the amount in foreign currency;

(c) the amount of any fees and charges applied for particular types of transactions.

(d) the exchange rate used for converting foreign currencies transactions.

When it is an electronic money instrument : the possibility of verifying the last five transactions executed with the instrument and the outstanding value stored thereon

184 Article 4.

Security obligations[185]:

The issuer is obliged not to disclose the holder's personal identification number; not to dispatch an unsolicited electronic payment instrument. And regarding a remote access payment he has the obligation to keep internal records to enable to trace the transactions, to rectify the errors and to ensure that appropriate means are available to enable the holder to notify the loss or theft of the electronic payment instrument or any other irregularity.

Burden of evidence[186]:

The issuer of an electronic payment instrument has to prove, in any dispute with the holder, that the transaction was accurately recorded and entered into accounts, and was not affected by technical breakdown or other deficiency.

The issuer must also keep for a sufficient period of time, internal records to enable the transaction to be traced and errors to be rectified.

This recommendation imposes therefore upon the issuer of electronic payment instrument a strong duty of care and technical obligation to keep records of all transactions.

Liability[187]:

The issuer is liable for the non-execution or defective execution of the holder's transactions, even if the transaction is initiated at terminals/devices or through equipment which are not under the issuer's direct or exclusive control, provided that the transaction is not initiated at devices/terminals or through equipment unauthorised for use by the issuer.

The issuer is liable to the holder of an electronic money instrument for the lost of amount of value stored on the instrument and for the defective execution of the holder's transactions, where the lost or defective execution is attributable to a malfunction of the instrument of the device/terminal or any other equipment authorised for use, provided that the malfunction was not caused by the holder knowingly.

---

185 Article 7.

186 Article 7 e.

187 article 8.

Therefore, it is important that the merchant makes a verification of the quality of the payment terminal he uses to be certain that he has got the right accreditation. Because if not , the liability of the issuer will not be automatically engaged.

The issuer is also liable for transactions not authorised by the holder or for any error or irregularity attributable to the issuer in the maintaining of the holder's account.

b Obligations of the holder[188].

Security obligations:

The holder has different security obligations, he must take good care for his electronic payment instrument, using it in accordance with the terms governing the issuing and use of such an instrument; take all reasonable steps to keep safe the instrument and the means which enable it to be used ; does not record his personal identification number in any easily recognisable form.

c. Liability of the holder :

The recommendation organises a specific system of liability. In case of lost or theft, the holder bears the loss sustained up to a limit which may not exceed 150 ECU up to the time of the notification of this loss or theft to the issuer.

This notification has a great importance, it is the turning point of the process. After the notification, the holder is exempted. But this mechanism runs only if the holder did not act fraudulently or with extreme negligence, in which case the limit does not apply.

Therefore, after the notification the holder is not liable anymore for the loss arising except if he/she acted fraudulently.

188 Article 5.

3. Directive on cross-border credit transfers[189].

The reason why we want to say a word about this directive is that in a few countries the payment made with a card can be considered as a credit transfers[190]. The directive is particularly interesting because it provides delay and a lot of obligations for the credit institutions such as obligation to refund in case of non-execution of transfers, obligations regarding time taken, information subsequent to a cross-border credit transfer...

The most interesting provision in our subject is the 'time obligation', because it could bring with it a lot of advantages for merchants which are dealing with European customers.

According to the terms of the Directive, the originator's[191] institution shall execute the cross-border credit transfer in question within the time limit agreed with the originator.

Where the agreed time limit is not complied with or, in the absence of any such time limit, where, at the end of the fifth banking business day following the date of acceptance of the cross-border credit transfer order, the funds have not been credited to the account of the beneficiary's institution, the originator's institution shall compensate the originator and this compensation shall comprise the payment of interest.

What remains is that it is really important to analyse each way of payment separately to tailor the right answer to the legal questions.

---

189 Directive 95/5/EC of the European Parliament and the Council of 27 January 1997 on cross-border credit transfers, OJ L 43, 14.2.1997. It is to be noted that this Directive has to be brought into force by the Member States by August 1999.

190 That opinion is defended in France and in Belgium see for example : M. Vasseur, " Le paiement électronique-Aspects juridiques ", in *J.C.P.*, 1985,I,3206.n°4 ; R. Trinquet, " Paiement par carte, l'irrévocabilité ", *Bancatique*, 1985, p.590 ; Y. Poullet, X. Thunis, " Réflexions sur le mouvement électronique de fonds ", in *La Télématique*, p. 258.

191 Article 2(h) provides that : 'originator' means a natural or legal person that orders the making of a cross-border credit transfer to a beneficiary.

VII. TAXATION ISSUES*

Introduction :

The tax issue in the field of electronic commerce in general is one of the most discussed at the moment. Different international bodies[192] have already issued comments, common positions, or recommendations. They are trying to keep the system coherent. But at present nothing has been clearly and unanimously decided, which means that the analyse provided in that deliverable could be completely changed by the future decisions of States, and organisations. It is why it seems important to pay a special attention to the changes which will certainly occur soon.

In this deliverable, we will focus us on the questions of VAT arising in the transactions between the different actors (see schema). The choice to speak more about VAT comes from the fact that as regards the ERMS operation, in the relationship between the rightholder, the operator of the ERMS and the final user, the question of direct tax is not so relevant.

But it remains important that each company carrying business on the Internet asks the question whether it has a permanent establishment in another country where it is carrying business. This criteria of 'permanent establishment' is the element determining the jurisdiction for direct taxation.

On the one hand, we will briefly analyse the general rules governing the permanent establishment (chapter I) in relationship with the questions raised by the ERMS.

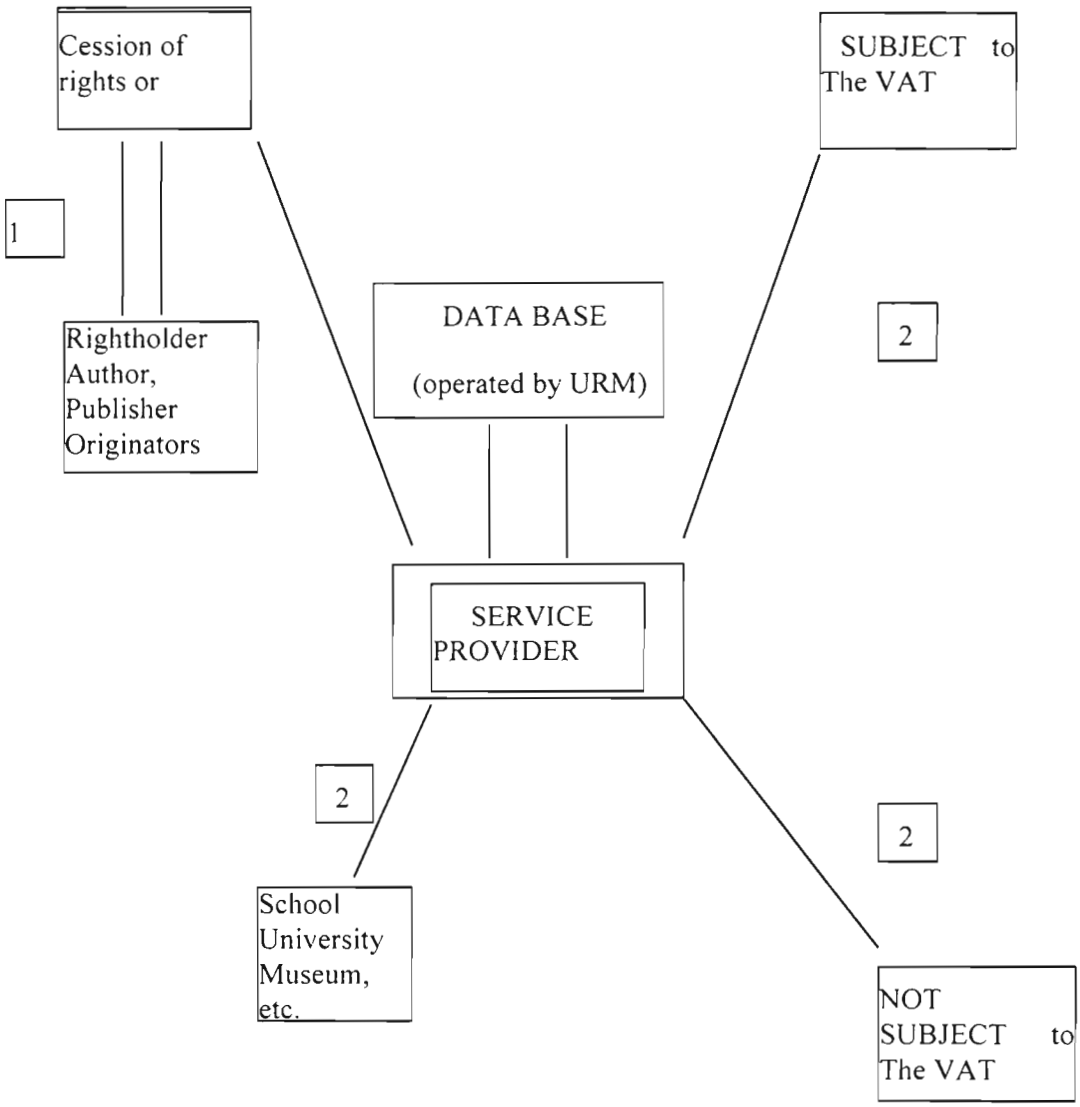
On the other hand, we will try to determine which VAT (chapter II) will be applicable, therefore, different questions have to be addressed. First of all it must be determined if the transaction is a delivery of goods or a supply of services (Section 1), the answer to that question will induce the applicable regime. Then, it will be necessary to know the categories the different actors behind to, and whether they are subject to the VAT or not; or, whether they have a specific status (Section 2). And finally it will be analysed where the transaction takes place, in order to determine which VAT is applicable, either the VAT of the country of the supplier or the consumer's country VAT (Section 3).

---

* Author : Laetitia ROLIN

192 Like the European Commission, the OECD, the US Federal Administration,..

The picture tries to summarise the different relationships arising during the transaction.



First of all, there is a license granted by the rightholder to the service provider on the works which will figure in the database (1). Then, the rightholder will put all the material in his database and sell the information to different end-users, private or professionals (2).

1. Direct Taxation Income.

The question to know if the company has a permanent establishment in another country arises because if it has one, it can be regarded as participating in the economic life of the source State to such an extent that it comes within the jurisdiction of the source state taxing rights.

The Double Taxation Convention on Income and Capital (Model Convention), issued by the Organisation of Economic Co-operation and development (OECD), provides in article 5.a definition of the concept as a fixed place of business through which the business of an enterprise is wholly or partly carried on.

The question whether a company carrying business has or not a permanent establishment in another country has to be examined in the light of the specific business carried. In the case of the ERMS, there are two kinds of business : the licensing of rights and the provision of access to a copyrighted application.

1.1. The licensing on works protected by the copyrights.

There is a specific article[193] on the royalties in the Model Convention on Double Taxation on Income and Capital (OECD). This article provides that the royalties coming from a contracting State (A) and paid to a resident from another contracting State (B) are taxable in that other State (B) if the resident is the effective beneficiary. According to the comments of the Model Convention[194], the royalties also cover the payments made in execution of a contract of licensing.

But the royalties will be taxable in the State where they come from if the beneficiary practise in that State an economical activity through a permanent establishment and if the work generating the royalties is effectively related to[195]. Nevertheless, all European

---

193 Article 12 §1 : "Les redevances provenant d'un Etat contractant et payées à un résident de l'autre Etat contractant ne sont imposables que dans cet autre Etat. si ce résident en est le bénéficiaire effectif.

194 Comments §8.

195 Article 12 §4 :"Les dispositions du paragraphe 1 ne s'appliquent pas lorsque le bénéficiaire effectif des redevances, résident d'un Etat contractant, exerce dans l'autre Etat contractant d'où proviennent les redevances, soit une activité industrielle ou commerciale par l'intermédiaire d'un établissement stable qui y est situé, soit une profession indépendante au moyen d'une base fixe qui y est située, et que le droit ou le bien générateur des redevances s'y rattache effectivement. Dans ce cas, les dispositions de l'article 7 ou de l'article 14, suivant le cas,

countries have entered bilateral conventions providing that the taxation of royalties will be ensured in the State of the recipient as an income.

1.2. The provision of access to a copyrighted application.

The case of the provision of access is more interesting because it concerns the parties to the online transactions i.e. the manager of the database (protected by an ERMS) and the customer. The problems arise from the fact that it has still not be solved whether a server or a database located in another country can be considered as a permanent establishment or not.

For example, the Austrian administration has decided that a British company has a permanent establishment in Austria when she sells information in Austria with the help of a server established in Austria of with the help of the server of an Austrian access provider on which the British company has rented space disk[196]. It remains that the comments of the authors go in different directions[197].

It depends also on what is really offered on the website. If the server only contains information on the product, if he only treats the ordering or only the payment, the server can not be considered as a permanent establishment[198].

The answer would be more difficult to give with certainty if the server is in charge of the whole transaction. In that case there is no unanimity among the authors and the commentators.

According to certain authors[199], there is no permanent establishment and their conclusion is based on the exception contained in article 5.4.a of the OECD Model Convention on Double Taxation on Income which provides that there is no permanent establishment if the fittings are only used to stock, expose or deliver the goods belonging to the company.

---

sont applicables".

196 Administrative decision, 28/08/96.SWI.1996.462.

197 L. De Broe, *"Commerce électronique international face aux principes traditionnels de la perception des impôts sur le revenu"* , in Fiscalité et Internet, Actes du Colloque du CEFI, Louvain-la-Neuve, 13 février 1998, p. 6.

198 L. De Broe , op. cit. , p 6.

199 P. Gliklich, S. Goldberg, H. Levine, Internet Sales Pose International Tax Challenges, Journal of Taxation, 1996, p. 327.

For others authors[200], the article 5.4.a is not a sufficient basis to declare that a server which operates the selling process in its entirety is not a permanent establishment.

According to the disparity of the answers given to the question it will be strongly recommended to the company carrying business trough server located in another State to inform themselves about the different positions of the local administration.

2. The VAT.

2.1. Qualification of the transaction.

According to the qualification which will be given to the transaction, the burden of the tax will be supported by one or another party. The reason is that there are different rules according to the type of transaction made.

There are two main categories of transactions which are the delivery of goods and the supply of services. Each of those main categories contains different sub-categories such as, in the case of delivery of goods, distance selling, delivery of goods with transport by the recipient, etc.

Having a look on the picture which summarise the different transactions (supra) in the commercial process of an ERMS, it appears that there are actually two different transactions : the first one is the licensing on the works figuring in the database, and the second one is the provision of access to the requested information stocked in the licensee's database.

a. The licensing.

The licensing on works protected by copyright (or other rights) is considered in the European Union as a supply of service as a lot of other intellectual services[201].

---

200 L. De Broe , op. cit. , p 7.

201 In the UK, VAT Act 1994, Schedule 5 : the transfers concerned are the transfer of copyright, patents, licences, trademark and similar rights ; advertising services : services of consultants and other similar services, data processing and provision of information : banking financial and insurance services, from 1/07/1997 the telecommunication services.

b. The supplies of information.

According to the doctrine, in most of the Member States, the supply of information is also considered as a supply of services. In Belgium, for example, according to the "Almanach TVA", the provision of information located in a database is also to consider as a supply of services. This answer has been confirmed by the Minister of Finances during a question time in the Parliament[202]. In the United Kingdom, the supply of information and the data processing are considered as 'intellectual services'[203].

Furthermore, the European Commission has issued a Communication[204] on Electronic Commerce and Indirect Taxation in which are explained the guidelines the Commission will follow to regulate this sector. In the Second Orientation, the Commission declares that all electronic transmissions will be considered as supply of services, because it is the European Union's politic to consider that goods which are ordered and delivered through the networks are services.

2.2. Place of the transaction.

The general rule is that taxable services are taxed in the tax jurisdiction to which the supplier belongs[205], but this principle is subject to a lot of exceptions. The reason of the exception is to limit the "distortion of competition caused by tax differentials between tax jurisdictions in relation to purchases by those who are not permitted to set off the input tax credit[206]".

In Belgium, in the case of the supply of service, the general rule is that the place of supply is the place where the supplier has established his economic activity or a permanent

---

In Belgium, the intellectual services cover among others. "la cession ou concession d'un droit d'auteur, d'un brevet, d'un droit de licence, d'une marque de fabrique ou d'autres droits similaires".

202 Bull. Q.R. S.O. 1996/1997n°76 01/04/97 p.10 292.

203 Geoffroy A. Key, *"International Tax Issues in Cyberspace : Taxation of Cross-Border Electronic Commerce"*, Intertax, Volume 25, Issue 4, p.142.

204 The Communication has to be considered only as an indication on what will be the tax orientation of the Commission's politic, nothing more.

205 S. Eden. "The Taxation of Electronic Commerce", in Law and the Internet. Hart Publishing, Oxford, 1997, p.155.

206 Idem.

establishment from where the furnishing is rendered or, if he has neither of those, it would be the place of his domicile or usual residence[207]. But there are several exceptions, among which the supply of intellectual services such as the furnishing of information through a database. In that case, the place of supply is the place of the recipient of the service if he is a taxable person and if he ordered the service for the purpose of his commercial activity[208]. And if the supplier of the service is established outside of the European Union the taxable person will pay the VAT to her/his administration and keep her/his right to deduction.

In the United Kingdom, the VAT may be chargeable on the provision of services if the place of supply is the UK. A UK customer who acquires certain intellectual services[209] may be treated as having been supplied with those services in the UK, even though the supplier may have no place of business in the UK.

In these circumstances, a recipient (subject to the VAT) of such services would be required to charge itself VAT on the 'imported service' under the "reverse charge" procedure. According to this procedure, the recipient is required to account for input VAT, instead of the supplier[210].

2.3. Influence of the status of the supplier of services.

The process of the reverse charge works only in two cases : where the supply is to a person who belongs outside of the European Union and where the supply is to a taxable person in another Member State and for the purpose of that person's business[211] In the contrary, the private person not subject to the VAT will pay the VAT of the supplier of services.

---

207 Article 21 §2 du Code TVA.

208 Code TVA article 21§3 7°

M. Dassesse, B. Vanderstichelent, Droit Fiscal II, Presses Universitaires de Bruxelles, 1998, p. 68, §87.

209 Value Added Tax Act 1994, Schedule 5.

210 S. Eden, "The Taxation of Electronic Commerce", in Law and the Internet, Hart Publishing, Oxford, 1997, p.156.

211 UK VAT Order 1992 SI 1992/3121, Art. 16.

Belgian Code on VAT, article 21§3,7°.

This table summarizes the different possibilities according to the status of the person and to his/her place of belonging.

Recipient / Supplier	**EU Taxable person**	**EU non taxable person**	**Non EU recipient**
EU Taxable person	Recipient's VAT if they are in different country and if the recipient ordered for the purpose of his commercial activity.(reverse charge)	Supplier's VAT	No VAT, but the supplier keeps the right of deduction
EU Non-taxable person	No VAT	No VAT	No VAT
Non EU person	Recipient's VAT if the recipient ordered for the purpose of his commercial activity (reverse charge).	No VAT	No VAT

Conclusion :

After the reviewing of the different questions raised in the field of taxation , we would make two recommendations. First of all, in the case of the direct taxation, it seems very important to ask for information to the relevant administration in all of the countries where the supplier of service is carrying business through a website, particularly if the whole transaction is made on the site.

Secondly, concerning the VAT, it seems that the international organisations and the States are decided to issue details about the applicable VAT to the Electronic Commerce. Therefore, we strongly recommend to the business carriers to keep informed about the possible changes in that field.

VIII. MODEL OF LICENCE CONTRACTS*

Foreword :

What follows constitutes Model Contracts or notices at multiple levels. Firstly, short notice should appear on the homepage of the Website. They don't constitute agreement since it is only information to be provided to the user on the conditions to use the copyrigthed application. Afterwards, a licence will be proposed to the user upon which he can agree by clicking on an icon. This first licence contract determine the general terms and conditions to use the copyrighted application. And finally, for each requested work component, an offer will be proposed to the user. If the user agrees upon the conditions, a new contract will be entered (this is the contract services drafted by Level 7). This contract simply resumes the fact that it is ruled by the general licence agreement entered with the user the first time he logs into the copyrighted application.

In all these proposed clauses, the text in italic character is the suggested text for the Model clause. An explanation of the rationale of the clause and of other options are provided in a normal character. Where some mentions are in brackets [ ], it indicates that it should be replace by the specificities of the project to which the Model applies (for instance name of the parties, title of the copyrighted application, etc...).

In this Model Contracts, we use the same terminology than that of the Business Model, a definition of which is to be found in the introduction of this deliverable.

These Model Contracts are aimed at an on-line operation of the ERMS. Nevertheless, it can be applied to off-line support.

---

* Authors : Séverine DUSOLLIER & Jean-Christophe LARDINOIS

Warning

(To be put on the homepage or front page of the copyrigthed application. Such warning should be available to the user at any time of the transaction via a hyperlink.)

1. GENERAL POINT

- *The service [copyrighted application] is provided under a license* (a hyperlink can be put here towards the text of the licence) *which binds you at each further transaction entered with [distributor] and therefore defines what you may do with the [copyrigthed application] and contains limitations on warranties and your remedies.*

IMPORTANT :

- *This system is protected by an ERMS (Electronic Rights Management System) whose copyright is enjoyed by [...]*

An ERMS is a technology enabling to electronically authorise the access to and usage of copyright applications and to manage their IPR (Intellectual property rights) or any other contractual rights.

- *All circumvention of the ERMS as well as the manufacture and selling of circumvention device will be prosecuted by the laws in force*

No part of content and/or services may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, or otherwise without the permission of the rightholder

2. PRIVACY

a. Object of such a notice

As the URM will be processing personal data, concern will have to be taken, when developing or deploying an ERMS, of the legislation on the protection of privacy[212].

As a consequence, will have to be adressed in this home page , **information**

- on the name and address of the URM (responsible of the processing)

- on the purpose of the processing, types of data, operations and third parties to whom the data will be transmitted (for instance, rightholders, content providers, etc...)

- on the existence of an access right for users

Proposed clauses :

The controller of processing is ... [name and address of the URM]

Personal data are collected and processed as regards as access to and usage of [the copyrighted work and applications]. The data collected are : [e.g., your name, your adress, the usage of the server you carry out, any personal data attached to the payment, etc...].....

The purposes of the collect and the process of data is the execution of this licence contract and the electronic management of rights.

Should other purposes for the processing be envisaged, it is needed to mention them clearly. It can be for instance for marketing purposes, for statistical purposes, etc...

Personal data might also be collected and processed with respect to unauthorised access to the copyrighted applications for purpose of proof of copyright and/or circumvention infringement

212 See title of the deliverable 4.2

The data will be transmitted to the following people for the purpose of the copyright management :

- ..... (for instance: distributor, collecting societies, rightholders)

The users will have the right to have access and to make rectification to their personal data.

3. CONSUMER PROTECTION IN DISTANCE CONTRACTS

a. Object

The following specific clause is to be applied only in case of consumer and may be included in this Licence whatsoever.

The following terms will therefore bind the parties only in the case the end-user meets the definition of the consumer.

In good time prior to the conclusion of this license, the consumer shall be provided with the following information :

(a) identity of the distributor or any other agent who will be regarded as the distant seller and in the case of contracts requiring payment in advance (see payment clause in the license hereinafter), its address

(b) the main characteristics of the services

(c) the price of services including all taxes (see related licence clause)

(d) the arrangements for payment, delivery or performance

(e) the costs of using the means of distance communication, where it is calculated other than at the basic rate

(f) the period for which the offer or the price remains valid

Such information should appear both in the licence than in each transaction screen.

LICENSE

(This license should be available to the user at any time of the transaction via a hyperlink)

IMPORTANT : CAREFULLY READ THIS NOTICE BEFORE ENTERING THE SYSTEM, THIS NOTICE SHALL APPLY TO EACH TRANSACTIONS

By clicking on the icon "I accept" you indicate your acknowledgement that you have read the following license and agree to its terms.

That license shall not therefore be denied validity or enforceability on the sole ground that the transaction has been entered electronically or by mouse-clicking

The license is concluded at the time and the place where the click-mouse constituting the acceptance of the offer is made available to the information system of the URM.

The URM will keep a complete and chronological record to store all the electronic transactions occurred

Such electronic records will have a comparable evidential value to that accorded to written documents

This license constitutes a general agreement between you and the [distributor] for the access to [the copyrighted application]. Access to each component and any further offer and transaction shall be automatically governed by this license.

A. ERMS LICENSE : The URM grants you a license to have access and to use [copyrighted application].

Each access/use will be defined at each request and as a consequence, the conditions and the price of it.

B. You are allowed to :

accomplish all the necessary acts for the use of the work component to which you have lawfully accessed to, within the limits defined hereinafter :

Such limits are to be defined by the distributor or rightholders according to the service or application offered. For instance the following should be provided at least

You are not allowed to :

1. make a subsequent permanent digital copy of the work component to which you have access to

2. communicate or make available to the public the work component to which you have access to

C. TERM: This license shall continue for as long as you have access to and use the offer set corresponding to each transaction

D. LIABILITY : The URM will not guarantee you against any problems relating to technical access, such as delays, technical problems and more generally, all circumstances and infrastructures that the URM can not control.

In case of dysfunction, the URM reserves the right to interrupt or temporary limit the access to the system.

E. PAYMENT : A specific price will be determined at each transaction. The following payment instrument are accepted

The methods of payment have to be defined in each project.

F. GENERAL : This licence is the entire agreement between the parties, supersedes any other agreement or discussions, oral or written and may not be changed.

This license shall be governed and construed in accordance with the law of ....

The competent jurisdiction will be ....

If any provision of this license is declared by a competent jurisdiction to be invalid, illegal or unenforceable, such provision shall be severed from that license and the other provisions shall remain in full force and effect.

Contract services screen

This part should appear in the contract services screen where a hyperlink to the general warning and to the licence in its whole should be provided.

This screen should include at least the following items :

- a description of the object of the contract (digital object ID and usage type should be sufficient)
- The Price
- A clause such as "*The licence agreed by you still applies to this transaction* " (hyperlink to the licence)

CONCLUSION AND RECOMMENDATIONS

From the foregoing, we might conclude that an overall consideration of the ERMS and other technical devices protecting IPR or access to networks is truly needed. The management of IPR in the future electronic environment is already possible on a technical level. Technology has brought some answers to the threats for copyright holders in open computer networks such as the Internet. But at the same time, this technology raises new threats and issues whose answers should be given by the law. National and international legislators have to make it clear whether an ERMS is entitled to wrap the public domain, what is the nature of the exceptions and whether they can be overridden by contract.

Our involvement in the Copearms project has enlightened certain current issues that the European and national legislators should address :

- *As regards the Intellectual Property Law:*

  The legislator, both European and national, should take into consideration the status of public domain in the Information Society either by preventing the access to the public domain from being restricted, either by setting-up a sort of universal service, as what has been done in the telecommunications, for public domain and cultural or informational content in general.

  The nature of the copyright exceptions should be particularly considered as it has already been done in the database and software directives. A number of exceptions reflecting fundamental rights and general interests should be made binding. This consideration should be accompanied by a proper attention to the consequence of such a binding nature to the technology and particularly to ERMS. It is not sufficient to provide that some exceptions are imperative, the ways for the technology to accommodate such obligations should be addressed. We have seen that the binding nature of some exceptions of the database protection could not be properly complied with by a technology such as an ERMS. The same issue would certainly arise from the mere assertion that the copyright limitations are binding.

- *As regards the legal protection of the ERMS:*

  The protection of the ERMS against any circumvention, defeat or removal of piece of digital information attached to content, should take place in general legislation regulating computer crime. In this framework, the IPR protection should not be the ground for such a defence which would be more legitimate and workable if related to unauthorised access to networks and computer hacking. In such legislation, the preparatory activities should be mainly prosecuted.

- *As regards the Validity and enforcement of electronic contracts:*

  The validity and enforceability of electronic contracts by process such as mouse-clicking should be addressed. As a principle such new forms of contracting should be valid upon requirements of a certain level of security and electronic recording. The use of digital signatures and TTP should be encouraged. A particular attention to consumer protection should also be stressed related to electronic contracts.

- *As regards the consumer protection:*

  The national legislators implementing the distance contracts directive should make it clear in what electronic forms the written confirmation of required information could be communicated to the consumer. The right of withdrawal should not be of application where copyrighted content is made available to the consumer.

- *As regards taxation law :*

  It should be made clear that the on-line providing of information or copyrighted content has to be considered as services for taxation and VAT purposes. The place of taxation for VAT and direct taxation should be clarified as well in order that the ERMS can be build in by taking into account a due tax rates.

A due protection of ERMS should only take place in such a clarified framework. The development of ERMS and any other technology aiming at protecting and managing IPR-content on-line is only at the beginning. Therefore, any regulation to rule or to protect such technology should take the time to carry out a deep and appropriate consideration of the brand-new legal issues implied by such devices. The legislators should particularly pay

attention to the risk that some technological measures used for protecting Intellectual Property Rights, beyond being a tool for a better protection of Copyright and Related Rights in the Information Society, substitute themselves to the law.

At present, such technological measures, such as ERMS technology, are still developing in an uncertain regulatory framework. Therefore, the developers are waiting for some legal solutions and certainties namely as regards the scope of IPR, the copyright exceptions, the validity of on-line contracting and the protection of their systems.

Such a legal intervention is a key prerequisite for a proper development of ERMS, hence for a proper management and protection of intellectual property rights in the Information Society