E-Commerce and Digital Content

Apol·lònia Martínez Nadal
Dr. in Business Law
Department of Private Law, University of the Balearic Islands,
Carretera de Valldemossa Km. 7.5, Palma, 07071, Spain
apollonia.martinez@uib.es

Antonia Paniza Fullana
Dr. in Private Law
Department of Private Law, University of the Balearic Islands,
Carretera de Valldemossa Km. 7.5, Palma, 07071, Spain
antonia.paniza@uib.es

Maria J. Iglesias
Head of the Intellectual Property Unit
Centre de Recherche Informatique et Droit - FUNDP
maria-jose.iglesias@fundp.ac.be

Contents

1 IDENTITY AND DIGITAL SIGNATURE IN THE ELECTRONIC ENVIRONMENT 3

1.1 Introduction . . . 3

1.2 The Spanish National Identity Document As A Tool For Identification In The Digital Environment. Regulation And Applications 4

1.2.1 Concept And Features: Traditional Instrument With New Features . . . 4

1.2.2 Effectiveness . . . 5

1.2.3 Procedure And Requirements For Issuance . . . 5

1.2.4 Delivery Of Electronic Identification Document; Voluntary Activation Of The Identification And Signature . . . 6

1.2.5 Validity Of Electronic Certificates, Causes Of Extinction; Revocation Procedure In Case Of Loss . . . 6

1.3 Other Forms Of Electronic Identification. Reference To The Electronic Identification Of Law 11/2007, On Electronic Access of citizens to public services . . . 7

1.4 International Initiatives: Action Of The European Union . . . 8

2 ELECTRONIC CONTRACTS 9

2.1 Regulation . . . 9

2.2 Protection Of The Minors In The Information Society: Advertising And Information To Minors . . . 10

2.3 Electronic Contracts and Minors . . . 12

2.4 Minors As On Line Social Networks Users . . . 12

3 DISTRIBUTION OF DIGITAL COPYRIGHT CONTENT 14

3.1 Copyright licences . . . 14

3.2 Distribution of digital copyright content through DRMs . . . 16

3.2.1 Introduction . . . 16

3.2.2 The legal framework for the protection of technological protection measures and rights management information systems . . . 17

3.2.3 The intersection between copyright exceptions and technological protection measures . . . 19

3.2.4 Use restrictions imposed by means of DRMs 20

Chapter 1

IDENTITY AND DIGITAL SIGNATURE IN THE ELECTRONIC ENVIRONMENT

by Apol·lònia Martínez Nadal

1.1 Introduction

One of the problems of electronic communications is authentication that involves the lack of assurance about the identity of the author of a message. Technically there are different electronic identification systems more or less reliable and secure. From simple systems as a simple "password" or key word identification to more complex systems based on biometric techniques (reading the iris, fingerprint, etc). Among these systems must also be mentioned the so-called electronic or digital signature based on asymmetric cryptography technique and used as a substitute for handwritten signatures; used in conjunction with digital certificates issued by certification authorities can produce the same or even better effects that handwritten signature, in order to authenticate and preserve the integrity of transactions and documents (in addition to achieving non-repudiation at origin).

These systems are technological solutions of information security that may be appropriate to address the risks of electronic communications solutions and perceived as necessary by the parties themselves, and which are becoming more accessible for the broad development, in recent times, of information security technologies, initially limited to very small areas such as defence and national security, or certain internal banking practices.

These technical solutions have even become necessary from a legal point of

view according to the legal requirements for authentication and identity assurance in the electronic environment currently existing in various fields, eg for the validity of electronic billing, or to the admissibility of electronic voting in commercial companies.Only in this way, applying appropriate technical solutions for authentication purposes, electronic communications, despite the disappearance of documents and written signatures, may give legal certainty to the parties involved.

From a legal standpoint, in Spanish law we can find the general regulation of electronic signatures in Law 59/2003, which includes the particular regulation of the Electronic National Identity Document. But this document is not the only identification system in the electronic environment taken into account by the legislator: the Law 11/2007 of 22 June, on electronic access of citizens to public services provided, as we shall see, different identification systems whose implementation and enforceability must be chaired by the principle of proportionality.

1.2 The Spanish National Identity Document As A Tool For Identification In The Digital Environment. Regulation And Applications

One of the great innovations of the Law 59/2003 on electronic signatures is establishing the basis for regulation of electronic national identity document. In particular, articles 15 and 16 are the basic rules. These basic rules are developed by Royal Decree 1553/2005 of 23 December, regulating the issue of national identity and electronic signature certificates.

1.2.1 Concept And Features: Traditional Instrument With New Features

The creation of so-called electronic ID makes available to the public certificates, ensure identity ot the users and provide the ability to sign electronic documents.

The new National ID document is configured as a document with a dual nature and dual functionality. Thus Article 1 ("Nature and functions") of RD 1553/2005 assign it the role of traditional identification and identification functions of the holder in an electronic signature and electronic documents. This is achieved by incorporating the traditional paper an electronic chip that incorporates the digital identity digital certificates and electronic signature keys.

With these new elements, electronic ID card is more than a traditional ID card: it is not simply a document with identifying function (through the relevant certificate) but also an instrument of electronic signature (to the extent that incorporates the signature creation data, ie the private key corresponding to the certified public key). So that in case of loss of traditional paper ID, you may try to supplant the personality of the owner but also have to forge his signature and handwriting, while in the case of loss of electronic ID will not

only be possible the impersonation of the owner by third parties but also (and without prejudice to establish security measures to prevent third party access to the private signature key) these third parties may make electronic signatures identical to those of the proprietor and there is not possibility, in this case, to differentiate one and other. Therefore, the significance of the possession and, in particular the loss of both identification document is not the same, hence the importance of proper custody by the holder, which must be properly instructed by government to respect.

1.2.2 Effectiveness

It is intended that an electronic ID has the same value as the traditional paper based identity card for identification purposes of the citizens. This is laid down in Art. 15.2 LFE, which provides:

> "Every natural or legal persons, public or private, will recognize the effectiveness of the national identity card to prove identity and other personal data of the holder as recorded in the same, and to prove the identity of the signer and the integrity of documents signed with electronic signature devices included therein".

Therefore, the electronic ID becomes an instrument of electronic identification generally accepted in Spain mandatory for any entity, public or private. The general validity of an electronic ID for all uses (office, business, individuals) is undoubtedly an advantage for citizens and avoid the possession of multiple identification tools. However, we must mention the doubts raised by that general use (not only administrative use but also, especially, commercial use) of electronic ID. The existence of a valid electronic ID for all purposes, without any qualitative limitation, can be inconvenient for providers of private certification services that are dedicated to the issue of certificates of a business. The coexistence of these private operators with a public certification authority that issues certificates highly reliable, acceptable for general use and probably with low cost to the applicant, may be a problem from a business standpoint; and from a legal standpoint, its impact on legal principles (of European Union origin) which establishes the free market competition for providers of certification services should be analyzed.

1.2.3 Procedure And Requirements For Issuance

The procedure and requirements for the issue electronic national identity document are established in art. 4 and 5 of Royal Decree 1553/2005. The most important aspect to highlight from these precepts is that it is essential to apply for and obtain an electronic ID the applicant's physical presence in an certification authority's office to issue this document. This is relevant because it allows face verification of identity of the applicant. And what is more important, you may qualify the certificate identifying him as a qualified certificate incorporated

under Law 59/2003 (essential requirement for the recognition of legal validity to electronic signatures ex art. 3 Law 59/2003).

1.2.4 Delivery Of Electronic Identification Document; Voluntary Activation Of The Identification And Signature

Electronic certificates as a tool for secure distribution of public keys can not be valid indefinitely. There are a number of conditions, technical (necessarily limited life of the keys), who provide the certificates have a limited validity period. And even must be attend to unforeseen circumstances that come to cause disability or early termination of the certificate (by revocation or suspension thereof).

From a legal point of view, different legal systems provide different periods of validity. The Royal Decree 1553/2005, in art. 12, also limits the validity of electronic certificates incorporated into the electronic National Identity Card to a maximum period of 30 months (within 4 years maximum allowed by Law 59/2003 to recognized certificates). The result is that qualified certificates incorporated into the electronic DNI will have less duration than the own electronic National Identity Card (which is, in general, 5 or 10 years or even permanently, depending the age of the holder, pursuant to Art. 6.1 Royal Decree 1553 /2005).

Precisely attending to this divergence of time, Art. 12.1 second paragraph provides that issuance of new certificates may be requested to be incorporated in the electronic identity card, since the ID has not expired. The normal extinction of certificate is due to the end of the period of validity; that event and its effects are regulated in art.12.2 of RD 1553/2005 governing inclusion in the list of revoked certificates (when the early revocation is not the same as extinction by end of the period of validity).

If, as we have seen, the extinction of the certificate does not imply that the extinction of the DNI, by contrast, the extinction of the electronic National Identity Card (DNI) involves the extinction of certificates, according to art. 12.3 RD 1553/2005. Finally, Art. 12.5 RD 1553/2005 establishes that in cases of loss, theft, destruction or damage of the National Identity Card (pursuant to art. 8.1), the holder has to communicate those facts to the Police Headquarters, in order to proceed to early revocation.

1.2.5 Validity Of Electronic Certificates, Causes Of Extinction; Revocation Procedure In Case Of Loss

With the new electronic Electronic National Identity Card (E-DNI), Spanish citizens have the possibility of use electronic signatures, which can give security to telematic administrative procedures and business transactions over the Internet.

The implementation of this E-DNI is advanced: in May 2009 the figure of 9,000,000 electronic identity card issued in Spain was surpassed. In addition,

the new electronic DNI has a more complete legal framework.

A different question is the effective use of this electronic ID instrument: by the moment, the real use is scarce, as evidenced by statistics from the Spanish Tax Administration Agency (AEAT) on the use of user certificates in the electronic filing of the declaration of the Income Tax for individuals. Specifically, in the 2008 campaign for 2007, there were a total of 3,738,594 telematic declarations, and only 2833 ot them used an electronic ID (source: http://aeat.es/usocerem.html). These data demonstrate the need of greater dissemination of information to citizens about the possibilities and applications of the new electronic identity card.

Precisely to address this situation, the Spanish Council of Ministers of March 16, 2009 approved an agreement to give new impetus to the electronic ID, with an additional investment of 13.92 million euros.

Also, as a measure that could need to increase the use of the electronic ID, the government is preparing an agreement with Asimelec (Spanish Association of Electronics and Communications) and Aetic (Business Association of Information Technologies and Communications of Spain) in order to promote new computers have a digital ID card reader.

1.3 Other Forms Of Electronic Identification. Reference To The Electronic Identification Of Law 11/2007, On Electronic Access of citizens to public services

Under Spanish legal system, the Law 11/2007 of 22 June, on electronic access of citizens to public services, recognizes, in its art. 1, the right of citizens to interact with government electronically. Therefore, the Law 11/2007 stipulates that governments not only can but must provide electronic access for citizens.

To exercise this right of electronic access, the issue of identification of citizens must be resolved. Under paragraph 2 of art. 13 of Law 11/2007, citizens can use the following electronic signature systems to interact with Public Administrations:

1. In any case, electronic signature systems incorporated into the National Identity Card for individuals. Electronic ID cards are an instrument of universal electronic identification for all dealings with government, as confirmed in art. 14 ("Uses of National Identity"): "Individuals may, in any case and universal, using electronic signature systems incorporated into the National Identity in relation to electronic government".

2. An advanced electronic signature systems, including those based on electronic certificates, recognized by the government. Therefore the law supports the use of advanced electronic signatures; according to the regulation and classification of the Law 59/2003 on electronic signatures this kind of

signatures are those that provide authentication and integrity, among other demands.

And, for these advanced electronic signature systems, art. 15 2 states that the "list of advanced electronic signature systems supported, in general, within each public administration, must be public and accessible electronically. This list includes at least information about the elements of identification used and, where appropriate, the characteristics of electronic certificates admitted, providers and the specifications of electronic signature that can be done with those certificates.

3. Other electronic signature systems such as the use of keys concerted with prior registration, information known to both parties or other cryptographic systems. These instruments would be include in the broad concept of electronic signatures with very different techniques with different complexity and security.

1.4 International Initiatives: Action Of The European Union

Finally, we would like to mention the existence of various international initiatives on electronic identification.

In this regard, the European Commission presented in 2008 a pilot project with a duration of three years which aims to ensure cross-border recognition of national electronic identity systems.

It also aims to facilitate access to public services in 13 of the 27 member states of the European Union (Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom), together with Iceland (EEA). The new system will allow citizens can safely identify and use the national electronic identity systems (passwords, ID cards, PIN codes and others) in the European Union level.

The implementation of this project will align and link existing systems.

Information about this initiative can be found in [3].

Chapter 2

ELECTRONIC CONTRACTS

by Antonia Paniza Fullana

The main problems on electronic contracts are analyzed in this report. The European and Spanish law are studied (Laws about Electronic Commerce; Distance Contracts; Financial Services and Distance Contracts, Consumer Protection Act; Data Protection Act). The main issues are: advertising and minors and online networks.

2.1 Regulation

- 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.
- Directive 2002/58/CE on Privacy and Electronic Communications.
- Directive 2000/731/EC on Electronic Commerce.
- Spanish Data Protection Act: L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Spanish Electronic Commerce Act: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Spanish Advertising Act: Ley 34/1988, de 11 de noviembre de 1988, General de Publicidad.
- Spanish Minors Act: L.O. 1/1996 of 15 January on the Legal Protection of Children.

- Law 17/2006 of 13 November, about the rights of children and adolescents in the Balearic Islands.
- Law 12/2008, of integral protection of children's adolescence (Comunidad Valenciana).
- Law 1/1998 of 20 April on child protection in Andalucia.

2.2 Protection Of The Minors In The Information Society: Advertising And Information To Minors

Issue of advertising directed at children can be analyzed from different points of view: advertising to children, characteristics of that publicity, data collected to carry out marketing campaign and personalized advertising... First point will be developed under this heading.

In Spain, Comunidades Autónomas can regulate the main subjects about advertising. For instance, Balearic Islands: article 30.47 Estatuto de Autonomía. Besides, they can regulate some aspects about consumer protection (article 30.47 Estatuto de Autonomía); domestic trade (article 30.42 Estatuto de Autonomía) and they can regulate some aspects about minors (article 30.39 Estatuto de Autonomía).

Rules implementing these aspects may be drawn above the main features of advertising can be studied: How should it be? Where are the limits? The Law 17/2006 of 13 November, about the rights of children and adolescents in the Balearic Islands as regulated in Articles 41 to 47 and in Article 49 and 50. It is intended to protect minors from two perspectives: as a recipient of advertising (for instance, as a consumer of information) and as the main character of commercial advertising (on this point from the perspective of the right to the image of minors).

Under this rule, advertising aimed at minors must adapt the language and messages at children, the representations of the products advertised must be genuine, must state the price, you can not make promises of goods or services involving compliance conditions not specified explicitly, and so on1. Although these standards must also be fulfilled on the Internet, we need an adaptation of advertising aimed at children with new technologies. For instance, a regulation of the use of banners, pop ups, those situations in which a single click downloads software or application or situations that may confuse the child about whether or not he makes a purchase. Also, we do not forget the easy availability of personal data. There are a general reference in the law for establishments that offer telematics services will have to install appropriate technical means to restrict access by minors to those pages that are harmful.

Law 12/2008, of integral protection of children's adolescence (Comunidad Valenciana) in its Article 72 states: "Telecoms operators must take the necessary legal and technical measures to ensure the protection of minors as users

telephony, television and the Internet over access to information, programs and services of violent content". This provision already covers both the technical and legal measures. As in the previous case, advertising to children must take into account the level of knowledge of the audience it addresses and the language and messages must be appropriate to the minor public and may not encourage discrimination or violence. Furthermore, advertising must be real with the right information and do not encourage consumption. In no case can be exploited minors confidence in parents, teachers or other people you trust. Moreover, Article 76 of the Act relates to child protection as a consumer and user referring to the defense of minors in abusive practices, adequate safety measures, etc.

Law 1/1998 of 20 April on child protection in Andalusia also refers in its Article 7 to the information and advertising to minors. Under this rule the government shall ensure that the media did not broadcast programs or advertisements against the interests of minors. Of particular interest is the mention of new technologies.

It is very important too the issue of information to minors. According to Legal Protection of Children Act have the right to seek, receive and use information appropriate to their development. According to the regional rules already cited should be clear information and taking into account the audience they are addressing. Additionally, do not encourage the purchase of a product or service. Under Article 50 of Law 17/2006, November 13rd, the treatment and rights of children and adolescents of the Balearic Islands, the government of the Balearic Islands will control the business practices that manipulate people under age for the covert sale of specific products.

On the other hand, code of conduct in Internet have regulated the questions about advertising and information to children. They try to guarantee the rights of the minors in Internet. The first step in this question is article 18 Electronic Commerce Act: codes of conducts will have particular regard to the protection of minors and human dignity and can be developed if it is necessary, specific codes on these matters. This is the case of Autocontrol code of conduct [1]: publicity in electronic media must not remotely moral or physical harm to minors and will therefore respect the following principles: the duty to identify the contents that are directed to adults, the advertising must not directly encourage minors to buy a product or service, "exploiting their inexperience or incredulity, or persuade their parents to purchase products or services. In addition, you can not exploit the special trust children place in parents, teachers or other people and should not be present to children in dangerous situations. Other questions in the Code of Conduct:

- To collect data or communicate with minors must take into account the age and knowledge of the persons to whom it is addressed.
- You can never collected data on the economic situation or privacy of other family members.
- The companies adhering to encourage minors to obtain consent from parents before providing your personal data on line, establishing effective

mechanisms for this technology.

- Parents or guardians may object to send advertising or information requested by the children in their care, addressing the person responsible for the file. And companies adhering to this Code will limit the use of data provided by children with the sole purpose of the promotion, sale and supply of products or services suitable for minors.

- Companies adhering to the code will support any efforts made by other agencies to help inform parents on how to protect online privacy of their children, including information about software tools and control access for parents to prevent children provide their name, address and other personal data.

2.3 Electronic Contracts and Minors

Some possibilities of verification on line the age of the person who use the services or who buy something... can be: to verify a credit card that the parent is the owner or sending an email to the parent to ask the consent retrospectively. The problems of impersonation on the internet have to try to avoid using formulas that minimize the risk by ensuring parental consent.

Code of conduct of Aptice [9] states that if a minor wants to perform a contract, the certified firm must require the user to verify their age as well as enough information to contact their legal representative. Furthermore, we should not exploit the vulnerability or lack of experience of children in order to contract certain goods or services.

2.4 Minors As On Line Social Networks Users

We can analyze the terms on the main on line social networks. Some aspects are very difficult to resolve, besides the international aspect must be taken in account.

FACEBOOK: Children Under Age 13: "*Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us through the form on our privacy help page*".

Children Between the Ages of 13 and 18: "*We recommend that minors 13*

years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet".

" *You will not use Facebook if you are under 13*".

Myspace: The MySpace Website is a general audience site and does not knowingly collect PII or Related Data from children under 13 years of age.

The first problem arises because the age limits as a person of 13 years need parental consent in order to provide valid consent in Spain. Another problem is the identity fraud and this question can be aggravated when the person is a minor: How can you control? The question is not easy. We can find any mention of the problem in the resolution on social networks of the 30th International Conference of Data Protection and Privacy, held in Strasbourg from 15 to 17 October 2008 that recommends that children should avoid giving the data from their homes or phone numbers. And also states that the default settings must be specifically restrictive when a social networking service is targeting to minors that very few users change the configuration. And the report of the Spanish Personal Data Agency on personal data privacy and security of information in social networks argues that because the vast of social network users may be minors propose that more authorities and associations lead joint initiatives to promote training among minors and parents about their safety with the investigation of technological possibilities to identify children who use these services. And this problem arises in two ways, in one hand when is the minor who enters their data on the social network, and, on the other hand, when a third party introduces, for example, photographs which the minor appears. (About minors and social on line networks: [5])

The problem about the advertising for the minors and the use of their data by the marketing enterprises are very important too. For children under 13 must also take into account the type of advertising that targets them. Every day we receive advertising more personalized. And this is possible thanks to data derived by companies and we must remember that they can not collect data from a child-according to the examples that have been exposed for 13 years without the consent of their parents and therefore may not be assigned to any company to conduct advertising campaigns. Problems that arise with clauses like this: " *When you publish content or information using the 'everyone' setting, it means that everyone, including people off of Facebook, will have access to that information and we may not have control over what they do with it*".

Chapter 3

DISTRIBUTION OF DIGITAL COPYRIGHT CONTENT

by Maria José Iglesias Portela

3.1 Copyright licences

From a legal perspective the on line distribution of digital content is done through contracts or licences. The so called End User License Agreements (EULAs) are usually attached to the digital content provided to the user. They contain the principles under which the use of the content is authorized by the provider. Digital content may be protected by copyright. Copyright traditionally refers to the protection of literary and artistic works[1]. It extends to the expression and not to the underlying ideas, procedures, methods of operation or

[1]Art. 2 Berne Convention, refers to "literary and artistic" works as "every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatic-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." This is a mere illustrative and non exhaustive list. So, copyright also protects other original works not cited in art. 2 such as maps, software, databases, films or multimedia productions. According to art. 2.5 compilations or databases may also be protected by copyright: "Collections of literary or artistic works such as encyclopedias and anthologies which, by reason of the selection and arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections". Vid also art. 2-5 WIPO Copyright Treaty (hereinafter WCT)

mathematical concepts as such[2] -the so called idea expression dichotomy-. At the same time, copyright only protects original works. The criteria and degree of originality required for copyright protection is not defined and may vary from one country to another and from one category of work to another [10]. In any case, the author of the work must enjoy some freedom to create, i.e. the work should be the author's own intellectual creation [3]. Accordingly, mere information and raw data are not protected by copyright, although the barrier between what should be considered mere information or data and a copyrighted work is not always clear and may vary a lot from one jurisdiction to another. Different from patents' rightholders prerogatives, copyright is an automatic right: it arises with the mere act of creation(-fixation) and it is not necessary to apply for it. In addition to moral rights, copyright grants the rightholders an exclusive exploitation right on the work. Exploitation rights last for the life of the creator plus 70 years [4]. Once this term is elapsed, the work falls in the public domain and may be freely used. Because the exploitation monopoly, the rightholders' authorisation is needed to make any use of the work -unless a copyright limitation applies. However, this principle of permission has been used as a tool to reconstruct the commons in the area of copyrighted works. As pointed out by Dusollier, licensing is now employed to promote a collective access to, and sharing of, intellectual resources produced and distributed through a logic opposed to proprietary exclusion [6]. This is clearly reflected on the creative commons webpage:

> "We use private rights to create public goods: creative works set free for certain uses." [2]

In the so called open access initiatives, exclusive rights are then being used as a means to enhance and facilitate access and sharing of copyrighted works. The open access schemes for scientific publications, software, films or music are based on licences attached to the copyrighted work. Although open licences vary a lot in nature, they generally tolerate the use of the work at minimum for non commercial purposes. Most of them include the so-called copy left clause. This clause requires that further use of the work, and in particular, any derivative work must be licensed under the same open principles or the same licence. More and more business models are built on open licences models.

Mainly in the case of proprietary licences, a conflict may exist when the EULA is used to prohibit actions that the consumer reasonably expects to have the right to perform when she acquires/licences digital content. Legitimate expectations may be based on Consumer Law and/on Copyright Law - i.e. in relation to the acts authorized by the copyright exceptions or in relation to the reproduction or communication to the public of works that are in the public domain. As regards copyright exceptions, only two European countries, Belgium and Portugal, explicitly consider copyright exceptions as imperative

[2] Art. 9.2 TRIPs and art. 2 WCT

[3] Art. 1 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

[4] Art. 26 Spanish Copyright Law

and mandatory[5]. The legal status of copyright exceptions in Spain is not clear, although there are arguments to consider that a general term forbidden an act authorized by the copyright law might be considered unfair, and then null and void [6]. A similar reasoning might be concluded in relation to the clauses prohibiting any reproduction or communication to the public of a public domain works. However, whether this reasoning could easily be applied in relation to the "acquisition" of digital files, its applicability to other business models, i.e. those on pay per use basis, would involve more difficulties[7] attending to the specific object of the contract. Unfortunately there is no case law on the issue. User expectations may be frustrated because of the implementation of use restrictions prescribed by the licences and/or by technological protection measures embedded into the material. In the next section, we will focus on the legal the technological protection measures.

3.2 Distribution of digital copyright content through DRMs

3.2.1 Introduction

Main objective of DRM systems is to control the use and dissemination of digital content by means of different mechanisms -i.e. cryptology, access or copy control techniques, identification and tracking systems- attached to digital objects. DRMs are an important tool to facilitate and enforce the protection of copyrights on digital contents as well as a relevant tool to manage the rights and, therefore, to distribute and commercialize copyrighted work and subject matter. Thus, the implementation of DRMs facilitates the development of new business models, in particular as regards the on-line making available of copyrighted work. In order to create a safe environment for these new developments, the World Intellectual Property Organisation (WIPO) adopted in 1996 two international treaties -the so-called Internet Treaties- granting a legal protection for DRMs. A bit later, the European and Spanish legislator have adopted legislation to comply with the WIPO mandate. But the European and Spanish Law go beyond the protection required by the WIPO treaties.

[5]L. Guibault proposes to introduce an item in the list of unfair clauses, according to which a non-negotiated contract would be deemed unfair if it departed from the provisions of the copyright act [8]

[6]Art. 83, Consumers and Users Act of 16 November 2007.

[7]S. Dussolier et at., Digital products in the acquis communautaire in the field consumer protection, Feburary 2009, Research report with the author, p. 10-12.

3.2.2 The legal framework for the protection of technological protection measures and rights management information systems

The legal protection of DRMs intends to prevent copyright infringements as well as to enhance the development of new business models for the online distribution of digital material. In the international Law, the legal protection for technological protection measures was granted by the so-called Internet Treaties -The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)- Art 11 WCT -and, in a similar wording, art. 18 WPPT - states that

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

Starting from this point, the Contracting Parties have different options to implement the obligations required by the WIPO treaties. Their discretion power mainly refers to the scope of the prohibited actions related to the circumvention of technical measures and to the type of technological measures to be protected. In relation to the first point, Contracting Parties may prohibit just circumvention acts, just preparatory acts or a combination of both[8]. As far as the technological measures are concerned, it may be distinguished between anti-copy or anti-access measures. The European Directive 2001/29[9] implements the WIPO obligation Treaties at the European level. At this point, the EU has opted for extending these possibilities to the maximum: it prohibits both circumvention and preparatory acts referred to anti-copy and anti-access mechanisms. The regulation of technological protection measures is covered by art. 6 Directive 2001/29/EC. This is, without a doubt, one of the most complex provisions in the Directive. In the first place, it imposes the Member States to provide adequate legal protection against the circumvention acts committed by individual persons having the knowledge, or with reasonable grounds to know, that are pursuing that objective (art. 6(1)), as well as against the so called preparatory acts (art. 6(2[10])). Immediately afterwards, art. 6(3) defines the technological protection measures as

[8] IVIR, Study on the implementation and effect in Member States' laws of Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society, Part I: Impact of Directive 2001/29/EC on Online Business Models, (2007), p. 73

[9] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10-19

[10] "Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

> "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC."

The protection is only granted for effective measures. In contrast with The Internet Treaties, the Directive clarifies when a TPM should be considered effective: "Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the right holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective." Thus, the concept of technological protection measures is linked to the right holders' will, and not to the prevention of a copyright infringement. Therefore the protection of technology is extended to uses traditionally beyond the exploitation rights[11]. Article 160 of the Spanish Copyright Law follows almost literally the wording of the Directive as far as the legal protection of the technological protection measures is concerned. In addition to the technological protection measures, art. 12 WCT -and in a similar way art.19 WPPT- deals with the obligations concerning Rights Management Information ?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?. According to the provision the Contracting Parties shall provide for 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: to remove or alter any electronic rights management information without authority; 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. A similar wording is contained in art. 7 Directive 2001/29 and art. 172 Spanish Copyright Law.

1. are promoted, advertised or marketed for the purpose of circumvention of, or
2. have only a limited commercially significant purpose or use other than to circumvent, or
3. are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

"

[11] S. Dussolier [7], pp. 131 y 163: "La protection devient plus large: c'est un critère subjectif (lié a la volonté de l'auteur qui la gouverne), et non plus un critère objectif (lié à la définition des droits et de leurs limitations)".

3.2.3 The intersection between copyright exceptions and technological protection measures

The WIPO treaties do not deal with the intersection between technological protection measures and copyright exceptions. Different from the WIPO treaties, Article 6 (4) Directive 2001/29 introduces a salvaguarde clause reducing the absolutism of the technology in relation to some exceptions. It establishes the basis to introduce national mechanisms that make possible the exercise of some exceptions if this is impeded by technological protection measures. These mechanisms shall be in place in relation to the so called *privileged exceptions*[12]. A specific regimen is stated for the private copy [13]. As far as the other exceptions are concerned, it seems that technology remains all its power. The general framework designed at the European level gives primacy to the will of the rightholders. According to art. 6(4) par. I, only if they do not adopt voluntary measures, the law must react. Therefore the European legislator is clearly for a subsidiary system. It should be read as an invitation to the market itself to facilitate the exceptions. These voluntary measures may be unilateral or derived from agreements between rightholders and other parties concerned[14]. In the absence of voluntary measures, the Directive 2001/29/EC imposes to Member States the adoption of appropriate measures to ensure the exercise of the privileged exceptions. But the European legislator does not specify what these appropriate measures could be[15]. The solutions provided in national regulations, without exhausting those advanced by the doctrine[16], are very diverse. Some states have recognized the beneficiaries a legal action before the courts, others have put in place an administrative procedure or looked at dispute resolution schemes (i.e. arbitrage, mediations or other alternative systems). In Portugal, rightholders are obliged to the legal deposit of the means to make possible the exceptions in the IGAC (*Inspecção-Geral das Actividades Culturais*)[17]. Indeed,

[12]Those referred in art. 5.2 a), c), d) and e); and in art. 5.3 a), b) and e) Directive 2001/29/EC

[13]Cfr. art. 6.4 II

[14]Directive 2001/29 mentions the parties concerned and not the users or their representatives. Then, these agreements, besides being concluded with the last ones, could be also negotiated with third parties not being users, i.e. content providers, software developers, etc... Indeed, in those countries where the national regulations just referred to the beneficiaries or their representatives when mentioning collective agreements, the agreements reached with third parties should be assimilated to the unilateral measures. See S. DUSOLLIER, Droit d'auteur et protection..., (2005), p. 169 [7]

[15]Directive 2001/29 mentions the parties concerned and not the users or their representatives. Then, these agreements, besides being concluded with the last ones, could be also negotiated with third parties not being users, i.e. content providers, software developers, etc... Indeed, in those countries where the national regulations just referred to the beneficiaries or their representatives when mentioning collective agreements, the agreements reached with third parties should be assimilated to the unilateral measures. See S. DUSOLLIER, Droit d'auteur et protection..., (2005), p. 169.

[16]The legal doctrine has advanced different proposals: an invitation to negotiate and reach contractual solution, the deposit of password or analogue copies, etc... See S. DUSOLLIER, Droit d'auteur et protection...[7], and quoted bibliography.

[17]Art. 221.1 Código do Direito de Autor e dos Direitos Conexos

some countries have created a kind of circumvention right in favour of users[18]. The Directive neither a priori clarifies, from a factual perspective, what an *appropriate means* could be. The Recitals do not give any clue, since they simple refer to the modification of an implemented technological measure[19] or to other means[20]. In order to prevent potential abuses, art. 6(4) par. III grants legal protection for any technological protection measures applied in implementation of the voluntary actions taken by rightholders, including within the framework of agreements, or taken by a Member State. Finally, art. 6(4) par. IV excludes from this complicated system those works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them. It means that works made on line available in virtue of subscription licences will fall out of this safeguard clause. The Spanish legislator has opted for granting the beneficiaries of some copyright exceptions a legal action before the courts when technological protection measures prevent them from enjoying the exceptions. This especial regime is also applied to database exceptions. Art. 161.4 explicitly refers to the private copy exception: it states that the right holder may establish a maximum number of copies to be made by the user. In this case, the user will not benefit from the salvaguarde clause contained in the precedent paragraphs. Copyright Law traditionally strikes a delicate balance between public and private interests. So, while it grants exploitation rights to the copyrightholders, it also includes some exceptions -the copyright exceptions- to these rights. Nevertheless, Directive 2001/20 as well as the Spanish Copyright Law fail to achieve this delicate equilibrium. The complicated system provided in art. 6.4 of the European Directive and developed in art . 161 of the Spanish Copyright law is very cumbersome and it will not guarantee in practice a fair exercise of copyright exceptions. Until this legal regime is modified, the main challenge for is to trust on the will of the rightholders and content providers -and to some extent on the will of DRMs designers- as regards the implementation of voluntary measures that make copyright exceptions effective.

3.2.4 Use restrictions imposed by means of DRMs

As indicated at the end of section 1, restrictions on the used of copyrighted content may be prescribed by the contract (section 1) or by technological protection measures embedded into the content. Technical restrictions may, for example, refer to the possibility of making copies of the content, its playlibility or interoperability, and the time they may last or be used. End-users must be clearly informed about the restrictions implemented by means of DRMs. This information is required by Consumer Law -imposing an obligation to inform

[18]This is the case in Denmark, where, if the rightholders do not comply in 4 weeks with the Copyright Tribunal order to make available to the beneficiary the means to enjoy the limitations, the user could circumvent the technological protection measures.

[19]Cfr. Recital 51

[20]Recital 51 in fine

consumers about the main characteristics of the products/services[21]. Lack of information on restrictions imposed by DRMs has been subjected to the scrutiny of European courts. Notably in France, several judgements have found that the sale of protected content without clearly informing on the existing technical restrictions as regards the playbility or interoperability of the content is unfair[22]. Also the European Commission has acknowledged that there is a need to set a framework for transparency of DRMs regarding interoperability, by ensuring proper consumer information with regards to usage restrictions and interoperability and considers that providing consumers with an accurate and easily understood labeling system on interoperability and usage restrictions, allowing them to make an informed choice will improve citizens' rights and provide for a sound basis for a wider availability of content online[23]. When the use restriction refers to acts authorized by copyright exceptions, end-users could make use of the ad hoc mechanisms foreseen in the Directive 2001/29 and in the Spanish Copyright Law (see supra section 2.3). But this mechanism will not apply if the restriction refers to unfair restrictions that do not relate to copyright law. This is the case in most European countries for the technical restrictions concerning the interoperability. Only France has foreseen in its Copyright Law provision facilitating the software interoperability. Competition Law may also be used as a tool to enforce the interoperability[24] of digital goods.

[21] I.e. the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, the Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, or Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Note that in 2004 the Commission launched the Review of the Consumer Acquis to simplify and complete the existing regulatory framework. During the preparation of the Proposal, the Commission considered extending the scope of the existing consumer protection rules (in particular Directive 1999/44/EC on consumer goods and associated guarantees) to cover agreements under which consumers get access to digital content. On 8 October 2008, the European Commission adopted a Proposal for a Directive of the European Parliament and of the Council on consumer rights COM/2008/0614 final - COD 2008/0196. The Proposal merges 4 existing EU consumer directives into one set of rules. At the same time it updates and modernises existing consumer rights, bringing them in line with technological change (m-commerce, online auctions) and strengthening provisions in the key areas where consumers have experienced problems in recent years - particularly in sales negotiated away from business premises (e.g. door to door selling), see [4] . For Spanish Law, see the obligations imposed under the Electronic Commerce Act for the on line distribution of digital content or under the Consumers and Users Act of November 2007.

[22] Court of Appeal of Paris, Decision of 4 April 2007, TGI Nanterre, 31 May 2007, and TGI Nanterre, 15 December 2006.

[23] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on creative content online in the Single Market, COM/2007/0836 final and the Commission staff working document - Document accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on creative content online in the Single Market. Following the Communication the Commission launched a public consultation and identified 4 main areas requiring EU action: availability of creative content, multi-territory licensing of creative content - , digital rights management systems (DRMs), and piracy / unauthorized file-sharing. Contributions to the public consultation are published on http://ec.europa.eu/avpolicy/

[24] See article L331-6 and L331-7 French Copyright Law.

Bibliography

[1] Código Ético de confianza online. http://www.confianzaonline.com. Artículo 29.

[2] "some rights reserved": Building a layer of reasonable copyright. http://wiki.creativecommons.org/History. last modified on 13 July 2007.

[3] Electronic identity: easy access to public services across the eu. http://europa.eu/, May 2008.

[4] European Commission. Proposal for a directive on consumer rights. http://ec.europa.eu/consumers/rights/, October 2008.

[5] Agencia Española de Protección de Datos. Tuenti se compromete con la aepd a implantar sistemas efectivos de verificación de edad y a depurar los perfiles de menores de 14 años. https://www.agpd.es/, 4 2009.

[6] Séverine Dusollier. Sharing access to intellectual property through private ordering. *Chicago-Kent Law Review*, 82(3), 2007.

[7] S. Dussollier. *Droit d'auteur et protection des oeuvres dans l'univers numerique*. 2005.

[8] Lucie Guibault. Accommodating the needs of iconsumers: Making sure they get their money's worth of digital entertainment. *Journal of Consumer Policy*, 31(4):409–423, December 2008.

[9] Asociación para la Promoción de las Tecnologías de la Información y del Comercio Electrónico (APTICE). Código de conducta. http://www.aptice.org.

[10] Adrian Sterling. *World Copyright Law*. Sweet & Maxwell, 1998.