LEGAL ASPECTS
OF THE INFORMATION SOCIETY

AUTHOR:
M. BAIN
M. GALLEGO
M. MARTINEZ RIVAS
J. RIUS

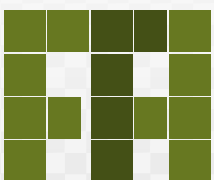FREE
TECHNOLOGY
ACADEMY

6

Legal aspects of the information society

Malcolm Bain
Manuel Gallego
Manuel Martínez Ribas
Judit Rius

Malcolm Bain

Malcolm is a lawyer and a partner at Id Law Partners, Barcelona, a law firm providing advice in intellectual and industrial property and information technology law. He specialises in the law applied to software and free content electronic commerce and personal data protection.

Manuel Gallego

Manuel is a lawyer graduated from Universitat Pompeu Fabra with a master's degree in Business Law. He currently works as a lawyer at the law offices of Fornesa, Prada & Fernández de Barcelona, specialising in commercial law: Company Operations, Commercial Contracting and New Technologies.

Manuel Martínez Ribas

Manuel is a lawyer and a Partner at Id Law Partners, Barcelona. He has served as coordinator and manager of European projects. Manuel is a regular conference lecturer in Barcelona, Madrid (ESADE, IESE, Abad Oliva, Fomento, Recoletos, Barcelona Chamber, Catalonian Technologies Institute, Internet Global Conference, Pompeu Fabra University, Universidad Politécnica Barcelona, Navarra University), Brussels, Paris (University of Paris), Fontainebleau (INSEAD), Darmstadt, Munich, Stockholm, Amsterdam, Milan, Rome, London and Zurich. He has authored several electronic commerce publications, digital tests, electronic agents, RFID.

Judit Rius

Judit has a bachelor's degree in Law and a master's degree in International Studies from Universitat Pompeu Fabra. She was also granted the La Caixa scholarship to study towards a master's degree in law, science and technology at Stanford University. A practicing attorney, she specialises in advising companies in the information technology and pharmaceutical sectors. She has collaborated in research projects with grants from the European Union and is a co-author of a study on the Law and E-Trade in Spain.

Preface

Software has become a strategic societal resource in the last few decades. The emergence of Free Software, which has entered in major sectors of the ICT market, is drastically changing the economics of software development and usage. Free Software – sometimes also referred to as "Open Source" or "Libre Software" – can be used, studied, copied, modified and distributed freely. It offers the freedom to learn and to teach without engaging in dependencies on any single technology provider. These freedoms are considered a fundamental precondition for sustainable development and an inclusive information society.

Although there is a growing interest in free technologies (Free Software and Open Standards), still a limited number of people have sufficient knowledge and expertise in these fields. The FTA attempts to respond to this demand.

Introduction to the FTA
The Free Technology Academy (FTA) is a joint initiative from several educational institutes in various countries. It aims to contribute to a society that permits all users to study, participate and build upon existing knowledge without restrictions.

What does the FTA offer?
The Academy offers an online master level programme with course modules about Free Technologies. Learners can choose to enrol in an individual course or register for the whole programme. Tuition takes place online in the FTA virtual campus and is performed by teaching staff from the partner universities. Credits obtained in the FTA programme are recognised by these universities.

Who is behind the FTA?
The FTA was initiated in 2008 supported by the Life Long Learning Programme (LLP) of the European Commission, under the coordination of the Free Knowledge Institute and in partnership with three european universities: Open Universiteit Nederland (The Netherlands), Universitat Oberta de Catalunya (Spain) and University of Agder (Norway).

For who is the FTA?
The Free Technology Academy is specially oriented to IT professionals, educators, students and decision makers.

What about the licensing?
All learning materials used in and developed by the FTA are Open Educational Resources, published under copyleft free licenses that allow them to be freely used, modified and redistributed. Similarly, the software used in the FTA virtual campus is Free Software and is built upon an Open Standards framework.

Evolution of this book

The FTA has reused existing course materials from the Universitat Oberta de Catalunya and that had been developed together with LibreSoft staff from the Universidad Rey Juan Carlos. In 2008 this book was translated into English with the help of the SELF (Science, Education and Learning in Freedom) Project, supported by the European Commission's Sixth Framework Programme. In 2009, this material has been improved by the Free Technology Academy. Additionally the FTA has developed a study guide and learning activities which are available for learners enrolled in the FTA Campus.

Participation

Users of FTA learning materials are encouraged to provide feedback and make suggestions for improvement. A specific space for this feedback is set up on the FTA website. These inputs will be taken into account for next versions. Moreover, the FTA welcomes anyone to use and distribute this material as well as to make new versions and translations.

See for specific and updated information about the book, including translations and other formats: *http://ftacademy.org/materials/fsm/1*. For more information and enrolment in the FTA online course programme, please visit the Academy's website: *http://ftacademy.org/*.

I sincerely hope this course book helps you in your personal learning process and helps you to help others in theirs. I look forward to see you in the free knowledge and free technology movements!

Happy learning!

Wouter Tebbens
President of the Free Knowledge Institute
Director of the Free technology Academy

Acknowledgenments

Contents

6. Cybercrime

Module 6
Privacy

1. Privacy – the protection of personal data
2. Basic concepts
3. General principles
4. Rights and obligations
5. Access to data and data transfers
6. Security obligations
7. Regulatory supervision
8. The legal framework for data privacy in other jurisdictions
9. Privacy in the sector of electronic communications
10. Conclusions: the impact of privacy on technological projects

Module 7
Open standards

1. Concepts
2. Standardisation processes – forums
3. Benefits of open standards
4. Controversies regarding open standards
5. The Future Way Forward?

Introduction to the legal aspects of the information society

Index

Introduction

Rumours began in 2003 and the first attack was staged in March: it was not the second Gulf War, but the offensive action taken by SCO, first against IBM, and later against the community of free software developers, over the code included in the then current kernel of the GNU/Linux 2.4 operating system.

This offensive brought to the surface tensions that were already being felt between the non-free software and the free software worlds. By 2000, it was reported that Microsoft had already made several critical statements in the so-called "Halloween documents" against GNU/Linux, an operating system that had began to acquire a share of the market that had until then been reserved to Microsoft (Windows) and several other companies distributing various non-free versions of Unix (IBM AIX, Oracle-Solaris).

Also in 2003, the European Commission drafted and the European Parliament debated a proposal for a directive to allow –or deny– the granting of patents on inventive computer programs and to determine the formal requirements for obtaining this protection. After the mobilisation of a large part of the software development community (not only those involved in free software, but also commercial software development companies and other stakeholders in the sector), in 2005, the same Parliament finally rejected the proposal – the first time in the history of the European Union.

This didn't stop Microsoft alleging, in 2007, that the GNU/Linux operating system was infringing upon some 283 of its patents, quoting a report that actually said that Linux "potentially" infringed 283 patents.

These "horror stories", so to speak, are indicators that the legal aspects of software in general and free software in particular are at the heart of current debates in the world of new technologies. These tensions are not merely technical issues relating to the stability, scalability or security of software, but rather derive from more basic issues in terms of who is the legitimate owner of the code included in the program, who may distribute such code, how payment is to be made and in what amount for a computer system considered free and available without limitations to date.

Moreover: these discussions form part of a broader debate on the freedom, culture and exploitation of immaterial works –which are defined as any program, movie, music, text or image in digital form– in the new information society. This debate incorporates several similar controversies including, for instance, the controversy regarding the downloading of music or movies on peer-to-peer (P2P) networks or the fight to achieve enhanced control by the owners of the rights to works broadcast over the networks and the "scope"

of such control: geographic (in what countries), temporal (for how long) and functional (what can be done with them), with special emphasis on digital rights management (DRM) systems.

The dilemma of the "non-free" industry lies in this: as new technologies allow for the mass copying and dissemination (and at a low cost) of intangible works protected by law (intellectual and industrial property rights), how can new technological and legal control mechanisms be established to protect the authors and owners of the rights to such work?

Facing a 40 year-old (or more) trend to extend the protection of copyright and reduce individual freedoms, and to extend patents to software functionalities – lobbied above all by the large entertainment, publishing and software companies – a form of protest movement has arisen claiming the freedom of culture and knowledge and their constitutive elements: music, written texts, visual works, computer software...

This protest movement is not the work of "long-haired revolutionaries". Quite the opposite, a team of law professors from the universities of MIT, Harvard and Stanford, for instance, has formed a centre for assisting in the dissemination of digital works (Creative Commons), whereby a new system of licensing copyrights has been established, allowing authors to carefully establish their level of control over the copying, modification and dissemination of their works.

A key component of this protest is the free software movement, led in its day – and for some, to this day – by the Free Software Foundation (FSF). Software is an intrinsic part of culture, not only as technological knowledge, but also as a par excellence means of access to culture and knowledge. Software is the foundation of the network of all networks, the internet, interconnecting commercial entities, citizens and public institutions. We should also consider that software is run on computers and makes computers run, and that computers are essential elements of the creation of knowledge and of today's social, commercial, scientific and educational relations.

References

- For more on SCO see the Wikipedia or the Groklaw sites.
- Halloween Documents are commented online.
- Proposed EU Computer Implemented Inventions Directive is described at the Wikipedia and the FFII sites.
- Linux patent claims are reported for example, at CNNmoney.com and eWeek.com.
- Digital Rights Management Systems are described at the Wikipedia site.

1. The free software movement and the law

Facing the restrictive legal framework where the default rule is "all rights reserved", and the tendency to apply this and corner scientific and technological knowledge by the large computer companies – perhaps led by large corporations as Microsoft, Oracle, Apple and Adobe, the free software movement (free and open, we are not distinguishing at this point) was born. This movement seeks to maintain and protect freedom in this sector, which is fundamental to modern society. This movement argues that the "non-free" trend is threatening to make us into the society of permissions – of "permissions, please" – where the owners of the knowledge must be asked for permission to use a work, which is granted under ever more restrictive, sometimes draconian, conditions.

Free software

Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it means that the program's users have the four essential freedoms:

• The freedom to run the program, for any purpose (freedom 0).
• The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.
• The freedom to redistribute copies so you can help your neighbour (freedom 2).
• The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

The Free Software Definition can be found at the GNU Operating System site.

However, what distinguishes the software sector from other parts of this more general protest movement is that the free software movement is based strictly and directly, to mark its protest, on current laws. Free software is distinguished from non-free software by how those same laws are used. Free software is not distinguished from non-free software by its quality or technology, although it is argued that it presents advantages in these terms, but by the copyright licensing regime. A free software licence does not contain the protection and control measures traditionally included in non-free software licences.

We should note that now, as of 2007 and 2008, several "traditional" software companies, which had used a "non-free" or "exclusive" model for the distribution of their products, are now embracing the free movement (or at least, the open source movement). Microsoft has published several programs under free licences, using its own licences, two of which have been approved "Open Source" by the Open Source Initiative. Sun (now part of Oracle) has released the Java environment under the GPL licence (and has purchased MySQL). Ya-

hoo! has purchased and now manages the Zimbra project. We must now see if these are actual commitments to development, based on free principles and ethics, or merely commercial strategies...

The development of office automation solutions (OpenOffice.org) as an alternative to commercial packages (mainly MS-Office by Microsoft) also involves certain legal aspects. Due to the dominance of the commercial packages in the business and domestic worlds, if a user of OpenOffice.org wishes to share text files, presentations or spreadsheets with others using non-free programs, it is essential for there to be interoperability between data formats. Nonetheless, these formats are often private program elements (non-free) and protected by copyright and even patent laws. In the absence of a public and open standard for such data format (such as ODF for documents), does a developer have the right to decompile or study the original code of non-free applications to be able to export or import files from a non-free source into the free application? Does obtaining a patent on an XML file export format imply the need to obtain a licence for such interoperability?

> Consider the patent obtained by Microsoft in the United States in February 2004 on XML scripts for Office 2003 and the recent approval of OOXML as a standard format. Will the Open Specification Promise made by Microsoft suffice to protect users from such new "standard"?

In 1998, Netscape opened the code of its Navigator to create a free version now managed by the Mozilla Foundation (with projects such as Firefox, Thunderbird, Seamonkey...). This radical decision not only led to the resignation by the director of technology (who could not see the strategic and commercial reasons behind it), but also instigated a heated debate on the terms and provisions of the new licence or, better yet, the licences. Netscape was forced to draft one licence for the initial Navigator (the Netscape Public License, MPL) and another licence (broader) for any future modifications (the Mozilla Public License).

Ultimately, the creation of free software, its modification and dissemination, software reengineering, interoperability, patentability, etc. are current issues, constantly present in any activity revolving around the core subject of this course on the legal aspects and exploitation of the information society, with a special focus on free technologies. These are issues that raise important legal questions. The legal aspects of a free information society are numerous and extremely relevant, as they condition all aspects of the process of creation, distribution and use of software and content.

Thus it is essential for anyone interested in creating, developing, distributing or using free software, to have solid knowledge of the relevant legal aspects and that is precisely the purpose of this course.

2. The free software model

The free software movement uses several arguments to defend its position and it is important to consider that such arguments have important legal impacts. To understand the free and open source software initiative, we consider it to be useful to briefly comment on these arguments.

2.1. The theory of the social genesis of understanding

The first argument used by the defendants of free software is philosophical-ideological. The basic principle is that knowledge as such does not belong to any one person, as all knowledge is based on earlier knowledge and is a copy, to a greater or lesser extent, of other ideas. Think of what Newton said about "standing on the shoulders of giants".

In other words, no one has ideas that have not been directly or indirectly influenced by social relations maintained in the communities of which they form part and if the genesis is social, the use must in turn remain social. The main function of the generation of knowledge is to improve society and, therefore, to reach the largest possible number of people.

If we were to consider software as knowledge, the argument made by organisations such as FSF seems simple. The most direct consequence of this philosophy of the social genesis of knowledge, from a legal viewpoint, is that the copyright law limitation against copying, using or redistributing software makes no sense, as it hinders the generation of new knowledge and does not allow for the accomplishment of its main purpose: returning to the community.

Example

In Spain, for instance, in 2004, the Regional Government of Extremadura launched LinEX, a broad program to promote the creation of distribution based on Debian GNU/Linux, for the purpose of installing it at all public education centres in the region. There are clearly technological and economic reasons behind this decision. However, the legal consequences are equally important: the use of free software provides the freedom to disseminate software among all citizens and residents, without the need to acquire another licence. The Regional Government may also easily modify these systems to adapt them to local needs, without requesting permission from the original owners –a considerable legal independence strategy. Educational centres benefit from the program, as they do not depend on suppliers (of software or maintenance and upgrading services). And they may open the source code of the applications installed for educational purposes (computer classes, etc.).

2.2. Greater dissemination

There is another reason, which could be considered the "pragmatic" reason. Free software supporters claim that the distribution of work under a free licence (in the sense of guaranteeing the aforementioned four basic freedoms to users) is the best way to obtain benefits from the publication of content, particularly for those that are not established developers or authors.

The argument is that those who truly win with the current restrictive copyright system are famous authors and middlemen, i.e., publishing houses. The rest of the creators live off the prestige that they receive from the works (and not from royalties), allowing them to provide "additional services", such as providing maintenance or consulting or giving conferences, courses, speeches, writing for newspapers, etc.

Continuing this argument, for most authors what is truly important, to increase their economic performance, is that their work reach the largest possible number of people. Along these lines, the conclusion they have reached, is that for an unknown author, the copyright system poses an obstacle to their reaching the public and benefiting from their creations. To counteract the impact of the legal framework, the works must be distributed under free licences, to ensure full freedom of redistribution.

Supplementary content
See Creative commons case studies for more examples.

2.3. Other arguments

We may cite other arguments used by the free software and content movement to support their position, all with legal impact or consequences:

- The enhanced dissemination of the work not only gives way to greater benefits, but also improves the work's quality (as mistakes are corrected, comments enrich the work, viewpoints are shared, etc.). To do this, it is necessary to provide the user with the right to modify and access the source code (when referring to programs). This is the philosophy behind Wikipedia, whose ranking in terms of quality is similar to that of the Encyclopaedia Britannica, in spite of the sometimes humble origins of its various contributors.

- The free software model is based on the participation of users, not only in the identification of errors, but also in terms of design and development. To do so, it is necessary to distribute the works (the software, for instance) as beta versions, with the freedom to install, use, test and contribute to the project or provide feedback (this is where the licence and lack of guarantees come in, as it is a beta version).

- The free software development model is more efficient: it is not necessary to reinvent the wheel, as the wheels –the software components, texts,

graphics, icons or photos– are available to be reused. This is possible in a digital world, as the "consumption" (use) of the digital object does not imply or require exclusive "ownership" of the product. Once again, this may solely be done with licences which allow free use (reproduction, distribution) in a non-exclusive way by the users.

3. Objectives of the course, key concepts

3.1. Objectives

Thus the main objective of this course is to provide the knowledge and necessary (legal) tools to be aware of the possible legal issues that are relevant in a Free Technology environment. In particular, it aims to help students understand the concepts and legal framework of free software and how to contribute and benefit from it in a safe and legal way.

We will look at the following concepts:

- The main legal reference framework for free software and technologies, and the information society in general, being:
    - **Copyright law** (known as "Intellectual Property Rights" on the European continent).

    - **Patent and trademark law** (also known as one of the "Industrial Property Rights).

    In the English and US legal framework, the concept of "Intellectual Property Rights" covers most forms of legal protection of intangibles, i.e. copyright, patents and trademark rights. This is confusing, as has been noted, and except when stated, we will avoid this term (see "key concepts").

    Concepts like existing legal systems of software protection – copyright, patents, trademark and key concepts like *copyleft* and free licences – will be studied to get a general background in those topics and to develop practical skills to use theme in different contexts.

- The **legal issues of online activities**, including ecommerce. The information society is a networked and "virtual" society, where many if not most activities take place online or are supported by online processes. We found it important for students to have an understanding of the legal issues raised by online activities – both as regards commerce and as regards citizen digital rights and obligations.

- **Privacy law** and how this impacts the processing of data and the defence of individuals' freedom and privacy in an ever more connected digital world.

- **Open Standards**, and how they are becoming more and more important in the context of software and format interoperability, cloud computing (where in fact the software doesn't matter, it is the interface and the format that do).

The principal legal framework for this work is European law, with examples taken from the laws of Member States (in particular England/Wales and Spain, where the author is qualified to practice). This work is under a free licence, thus examples, corrections and comments from other jurisdictions are welcome. Some non-authoritative references are also made to the US legal framework, mainly for comparing and contrasting approaches on how to regulate the Information Society.

3.2. Some key concepts

Any approach to the subject of the legal issues of the Information Society and free software and content implies facing a multitude of different definitions and terms. To unify criteria, in this section we will list some of the main concepts of the course and propose the definition that the authors will be using when referring to them.

By **intellectual property**, author's rights or copyright, we are referring to the system of protection of original, literary, artistic or scientific creations, which include software, and which reserve to their owners the rights to reproduction, transformation, distribution and public communication (upload to the internet) (see Module 2 for further details).

By **industrial property**, we refer to the legal system protecting the use or exploitation of distinguishing signs identifying products or companies (**trademarks**), inventions (**patents**) and confidential information of economic value (**industrial secrets**) (see Module 3 for further details).

A user **licence** is the legal instrument used by the owner of a work (software or other content) to grant permissions to third parties to use such work, in exchange for an economic remuneration or not.

Regarding the nomenclature relating to free and open source software licences in a broad sense, we shall use the following terminology:

- **Free software and free licence**: any licence respecting the four freedoms, thus allowing for its reproduction, distribution and modification, and granting access to its source code.

- **Open source software and open source licence**: software conforming to the guidelines of the definition of open code software (OSD), largely "synonymous" with free, but with another perspective (more commercial, more oriented to the access to its source code).

- **Copyleft software and copyleft licence**: applications and licences distributed with a copyleft clause, which may be strong (as the GPL) or weak (as the LGPL or the MPL).

- **Non-free or proprietary software**: applications distributed under non-free licences.

Intellectual property: authors' rights and copyright

Index

1. Intellectual property: authors' rights and copyright

Intellectual Property Rights, or IPR, are a series of rights that protect intangible (intellectual) works of human creation. While the term *IPR* in Anglo-Saxon countries confusingly covers several types of rights, including Authors' rights (copyright), patents and trademarks, in the continental tradition, IPR is limited to **Authors' rights, or copyright**, with the concept of "*Industrial Property Rights*" to cover other types of rights.

In this Module 2 we look at IPR in the continental tradition, Authors' rights, and its special relationship with software, while Industrial Property Rights are covered in Module 3.

1.1. The traditional concept of Authors' rights

Authors' rights is a legal term describing the certain specific rights granted to creators in their original works. In the legal system of most English-speaking countries, the term *copyright* is used, as we shall see later. In this section we shall see how the law establishes and regulates these rights.

Neighbouring rights

In the general theory of Authors' rights, there are also certain rights attached to a work that are granted to certain persons who are not authors, such as interpreters and performers on the one hand, and producers, broadcasting entities on the other. Thus a recorded musical work (e.g. a song) will be concurrently protected by several different rights:

- The authors' rights of the composer of the music and the lyricist.

- The performers' rights of the singer and the musicians.

- The producers' rights of the person or corporation which made the recording.

1.2. Origin of Authors' rights/copyright

Protection by Authors' rights stems from the historical moment when works were initially exploited economically by reproduction in hard copies. First, by medieval copiers and, especially, further ahead, with the appearance of the printing press. Publishing houses, as a whole, benefited directly from the invention of the press, as works were transformed into commercial objects that could reap them economic benefits. However, at the same time, the use of the

press simplified the reproduction of the works by third parties and publishers exerted pressure on lawmakers to obtain protection and secure their returns. By doing so, the first objective of Authors' rights/copyright was to regulate and protect publishing houses and presses by granting privileges, although they were also used by governors to control and censure works.

Origin of copyright

It seems that the first law on Copyright was the English Statute of Queen Anne (1710), which granted publishers exclusive rights to print and distribute their works for a limited period. These rights evolved over time towards greater recognition and protection of the actual author's rights in his/her creations, leading to the 1889 Berne Convention commented below and today's framework.

The evolution of Authors' rights/copyright bears a direct relation to their extension to new types of works and greater time periods, and the adaptation of the rules to the characteristics inherent in each type of new work that has been granted protection. Adapting Authors' rights/copyright to computer programs and to new technological means of broadcasting works has generated an unprecedented revolution in the traditional legal framework of Authors' rights/copyright.

1.3. Authors' rights or copyright?

We have used the term *Authors' rights/copyright* when we refer to the generic concept of the legal protection of works of authorship. The expressions *Authors' rights* and *copyright* are often used as translations of the same concept, however this dual denomination responds to two different conceptions of these rights that coexist today.

Simply put, the system of *Authors' rights* is more personalised and protects creations as extensions of the author's persona. On the other hand, the *copyright* system of Anglo-Saxon countries is more collective and tends to protect the economic interest in a work so as to encourage authors to create more, as a general-interest benefit for all.

Nowadays, there is a high degree of coincidence in the regulation of the two legal philosophies, due in great part to the internationalisation of intellectual property law and the harmonising function of international treaties on the matter. There are nonetheless some relevant differences, such as, for instance, in relation to the moral rights of authors, which we develop later on. In this text, we will use the term interchangeably, except where specifically indicated.

Copyright

If we wish to study the copyright system, we must focus in most part on the study of the United States legal system and the British legal system. In the United States, the most important copyright legislation applied to software is based on the Copyright Act of 1976 and the Computer Software Copyright Act of 1980. In the United Kingdom, the legislation currently in force is the Copyrights, Designs and Patents Act of 1988. These laws consolidate the legal provisions contained in several laws and case law.

1.4. Regulatory framework

In this section, we will briefly review the main legal frameworks providing the protection of Authors' rights, beginning with an international perspective and including European and national regulation.

1.4.1. Authors' rights at international level

The international framework for the protection of Authors' rights is made up of certain *international treaties* or *conventions* (treaties between countries mainly aimed at harmonising the legal regime) and certain *international organisations*, who monitor and develop new laws, among other functions. Let us start with the organisations.

- Organisations.The most important source of regulation of Authors' rights at the international level is now the *World Intellectual Property Organization* (or WIPO). Created in 1967, WIPO is a specialised agency of the United Nations whose main purpose is to develop an international intellectual property system rewarding creativity, fostering innovation and contributing to economic development, while at the same time protecting public interests. As such, it sponsors international treaties to harmonise the legal framework and remove barriers to the exploitation of works.
Another international organisation interested in Authors' rights is the *World Trade Organization* (known by its initials WTO), an international organisation in charge of the rules governing trade among countries. The WTO began to show interest in Authors' rights in the mid nineties, due to the growth in international trade in services and works susceptible of copyright protection.

- Treaties/Conventions. The first and foremost treaty on Authors' rights is the **Berne Convention for the Protection of Literary and Artistic Works of 1886**, with its most recent revision having been drawn up in 1979.
The Berne Convention is based on three main principles:
  - National treatment. Works originating in any of the contracting states must receive in each of the other contracting states the same protection as granted to the works of their own citizens.

  - Automatism and simplicity. Protection shall be automatic and shall not be subject to the compliance of any formality.

  - Moral rights. The Convention encompasses moral rights, i.e., the right for an author or his/her family to claim authorship of the work and to oppose any damage to its integrity.

The Berne Convention establishes the basic framework for Authors' rights, including the works that are protected, the scope and duration of rights and their limits, and certain specific provisions for developing countries. Chronologically, the next international treaty related to IPR is the **Agreement regarding the Trade-Related Aspects of Intellectual Property of 1994**, known by its acronym "TRIPS", sponsored by the WTO (see above). The agreement covers various broad issues such as how basic principles of the trading system and other international intellectual property agreements should be applied and how to give adequate protection to intellectual property rights. It also regulates how countries should enforce those rights adequately in their own territories and how to settle disputes on intellectual property between members of the WTO.

The most relevant contributions made by the TRIPS Agreement as to Authors' rights in the information society are:

– It compels signatory states to observe the provisions of the Berne Convention, with the exception of the requirements pertaining to moral rights.

– It protects computer programs as literary works, and outlines the protection for databases. For the signatory states of the TRIPS Agreement, the provisions of the Berne Convention are applicable to computer programs, regardless of whether they are signatories of the Berne Convention.

– It imposes upon the signatory states the obligation to grant the owners of Authors' rights to a computer program the right to authorise or prohibit the rentals of its products.

The legislative work at the international level did not end with these two treaties, and in 1996, two new treaties were subscribed under the WIPO framework, to adapt Authors' rights to the technological evolution, mainly the internet: the **WIPO Copyright Treaty** (WCT) and the **WIPO Treaty on Interpretation or Performance and Phonograms** (WPPT).

The WCT entered into force on 6 March 2002 and provides protection to authors of literary and artistic works, including original computer programs and databases. As we shall see, the European Union and the United States have pioneered the application of the provisions of this treaty in adopting the Copyright Directives in the European Union and the Digital Millennium Copyright Act (DMCA) in the United States.

The most relevant aspects of the WCT are:

– It universalises the Berne Convention and redefines its concepts within the new technological context, guaranteeing to rights holders that their rights will continue to be protected when their works are disclosed through new technologies and communication systems, such as the internet, creating new rights applicable to the internet environment.

–   It introduces the legal protection of the technological measures of protection, which we will comment on later.

Complete texts of the treaties

The complete text of all WIPO treaties and a list of their signatories are available on its website. The complete text of the TRIPS Agreement, along with its signatories and an explanation of its provisions, is available on the WTO website.

1.4.2. Authors' rights/copyright in European Law

Traditionally, in Europe, Member States have regulated intellectual property (copyright), leading to a huge casuistry in the regulation of the subject. Nonetheless, at this time, the centre producing legislation on intellectual property in Europe is no longer formed so much by the states as it is by the European Commission.

The function of the European Commission is complex inasmuch as, besides harmonising national legislations in the matter (where the copyright based system coexists with the Authors' rights system), it must attend to the international commitments acquired mainly, as we have seen, within WIPO and WTO.

The European regulations on Authors' rights and computer programs is based on **Directive 91/250/CEE** of the Council, of 14 May 1991, regarding the legal protection of computer programs, modified by Directive 93/98/CEE of the Council, of 29 October 1993 and restated in 2009 by **Directive 2009/24/EC** (the *Computer Programs Directive*). This Directive establishes that computer programs shall be protected by Authors' rights as literary works, as provided by the Berne Convention.

As regards Authors' rights more generally, **Directive 2001/29/CE**, of 22 May 2001, was adopted, regarding the standardisation of certain aspects of Authors' rights and neighbouring rights in the information society (the *Copyright in the Information Society Directive*, of EUCD). This new Directive seeks to bring all current regulations up to date, complying with the commitments assumed under the WCT. The negotiation of this Directive was controversial and implied a protracted debate on how to regulate copyright in a digital world.

The **Principles of the Copyright in the Information Society Directive (EUCD)** are as follows:

•   It broadens the concepts of reproduction and public communication (now including the right to make the work available to the public, e.g. by internet download), applied to all works, including software and to the complementary documentation distributed over the internet.

• It established legal protection for technological protection measures (TPMs – see below).

Finally, **Directive 2004/48/CE**, of 29 April 2004, regarding the enforcement of intellectual property rights, establishes harmonised measures, procedures and resources required to guarantee the respect for intellectual property rights within the EU, including rights of entry, seizure, injunctions and awards for damages.

Additionally, databases are granted protection under a special system with rights parallel to Authors' rights under **Directive 96/9/CE**, regarding the legal protection of databases (see below).

These Directives harmonise to a certain extent (but not fully) the Authors' rights/copyright regimes of EU Member States, providing broad brush similarity between the national legal regimes. There are notable differences, particularly between copyright and Authors' rights regimes with respect to fair use and moral rights, as we will see later.

• **National law**

  At national level, these international treaties and, in the EU, Directives have been implemented or legislated via statute. Without going into the complexities of international private law, it is important to remember that copyright law is national law, for while the protection is "international", courts apply the law of the country to works created in that country and disputes arising there in relation to other works.

  Recommended links

  • Spain: Ley sobre la Propiedad Intelectual.
  • UK: Copyright, patents and designs Act 1988.
  • France: code de la propriété intellectuelle, codified in laws of 11 March 1957 and 3 July 1985.
  • Germany: German copyright law or Deutsches Urheberrecht is codified in the Gesetz über Urheberrecht und verwandte Schutzrechte (abbreviated UrhG).

2. Protected works

In this section we shall attempt to understand the specific object of protection under Authors' rights (generally speaking, i.e. including thus copyright), especially as regards their applicability to software.

2.1. Works

Authors' rights protect or grant rights over "works". A work may be defined as the formal expression of an idea or feeling wished to be communicated to the public, expressed by any means or in any form, whether tangible or intangible, known now or invented in the future.

The type of work covered by Authors' rights or copyright includes **literary, artistic and scientific works**, including therefore novels, poems and plays, paintings, reference documents, newspapers, movies and audiovisual works, musical compositions and choreographies, sculptures, photographs, architectural works, advertising, maps and technical drawings, computer programs, databases, and many more works.

It is essential to understand that protection by Authors' rights cover the form, the container, the expression of the creative idea, but not the content or idea in itself. Neither the subject of inspiration (facts, dates...), nor ideas are protected by Authors' rights.

Computer Programs

A "computer program" is not defined, but we can use the following definition, variations of which are used by several EU Member States: *a sequence of statements or instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a machine-readable medium, of causing a computer (a device with information processing capabilities) to perform a task or achieve a particular result.* [WIPO Model provisions on protection of software, 1978/restated 1991]. Under the Computer Programs Directive, protection is extended to the preparatory design material, but not to certain interface information required for interoperability.

To understand the legal protection of software –as any other work susceptible of protection by Authors' rights– we must take into account the characteristics of its protection:

- Only the expression of a computer program is protected, the source and object code, not the ideas or algorithms they implement.

- A program is protected as an intangible good, regardless of the medium in which it is embodied.

The definition and scope of protection of computer programs means that all stages of preparation of a program are covered, from the time that there is an initial description, in graphic form (flowchart) or verbal form (recorded), sufficiently detailed to determine a set of instructions. It includes the expression in any programming language and also covers the series of instructions in semiconductors (microcode and firmware).

Accordingly, Authors' rights mainly protect the following elements of software:

- The computer program itself (source code, byte code, object code).

- The preparatory documentation, including architecture documents flowcharts, data models, UML diagrams, etc.

- User manuals and technical support documentation.

- Human interfaces, including graphic elements, sounds, fonts and other audiovisual elements.

2.2. Requirements for protection

To be susceptible of protection by Authors' rights, a work must meet certain conditions that may be summarised as follows: "works that are the original creations of man, expressed by any means or in any medium". Three conditions therefore apply:

- **Creation by man**. The program must be the fruit of the intellect of an author, as a consequence of his/her activity.

- **Expressed by any means and through any medium**. Intangible property requires an instrument or means of being perceived by the outside world. Therefore, works must be contained in a tangible or intangible means of expression, either known now or invented in the future. For software, the means of expression may be a hard drive, a diskette or CD-ROM, flash card, etc.

- **Original**. To be protected, works must be original. Merit or quality, destined use, degree of manufacture, lawfulness or unlawfulness and priority in time are all meaningless.

> **Supplementary content**
>
> Computer programs created by machines are generally not deemed susceptible of protection, with the exception of compiled software (created by a compiler), which is assimilated to software created by the person who configures and runs the compiler.

It is not easy to define originality. Indeed, it constitutes the most disputed matter over recent years in the continental tradition. The most orthodox tradition of the system of Authors' rights requires a "trace of persona or personality" of the author, although there is no unanimity in national legislations in terms of the degree of originality that may be required.

The test of the originality of a work tends to have two aspects: the first is that the work must be original of the author, in the sense that it truly should have been created independently thereby, not copied from other work; the second is that the work must contain enough creativity to not be susceptible of being considered something mechanical.

> In software, it is difficult to define when originality exists, as it is a utility creation, where sometimes there is little room to manoeuvre. A low-level criterion has been chosen and, in general, it is deemed sufficient for the software to be the result of a personal effort, i.e., that it not be a copy, for it to be considered original.

The copyright system generally requires a lower level of originality and solely requires that the creation should be the result of a personal effort, i.e., that it should not be copy. To the extent that the origin of the software may be attributed to the author, i.e., that it has been created independently and has not been copied from other works, it would be considered original.

2.3. Author's rights and software

Initially, computer programs were not marketed separately, as they were sold with the hardware and their protection was confused with that of the overall product sold, the computer (a phenomenon known as bundling, which has once again acquired importance with mobile devices and other such items). Furthermore, there were no technologies that could be used to copy them or use them outside of the computer in any general way, so there was no great concern for their protection.

The need for protection began to be seen in the late seventies, when, by reason of the United States antitrust legislation, IBM was forced to separate its hardware and software businesses. Consequently, computer programs began to be marketed in separate mediums and the autonomous protection of this technology, extremely vulnerable to copy, was warranted to protect the investments made in its creation and also as a means of encouraging the dissemination of computer programs to larger numbers of people.

Supplementary content

In the United States, for instance, a work is required to be incorporated in a tangible means of expression, from which it may be perceived, reproduced or communicated by any means, whether directly or with the aid of a machine or device.

History

The feeling of a need to protect computer programs gave way to a debate in terms of the most appropriate legal means of doing so:

- In the beginning, the position was sustained that programs could be subject to protection by the legal precept of patents (the computer program as an invention), and this was upheld by the case law of the United States on several occasions. Nonetheless, in the late sixties and early seventies, various national lawmakers and international treaties began to reject the protection of software by patent. Consequently, more industrialised countries (subject to great pressure by large computer companies) sought alternative means of protecting their software.

- A possibility arose to create specific or "*sui generis*" protection (the computer program as a new type of creation) with a duration of four to nine years and mandatory registration, although such initiative never took off (see, for example, the WIPO Model Provisions for Software Protection of 1978 and the Draft International Treaty for the Protection of Computer Programs of 1983).

- Another possibility was also seen to protect software through the precept of Authors' rights and copyright (the computer program as a literary work), and this was the successful option.

Finally, a generally accepted principle was reached whereby **computer programs would be protected by Authors' rights**, while the hardware using computer programs or other inventions relating to such programs would be protected by patents.

The choice of the system of Authors' rights for the protection of software was based in good part on the advantages posed by the protection of any work with the Authors' rights system:

- Automatism. The right of the author derives from the mere original creation. No novelty is required.

- Simplicity. The protection of a work does not require registration at registries, the compliance with formalities or the prior examination of conformity.

- Economy. The protection does not require substantial economic investments.

- Coverage. The protection is extended to the accessory documentation.

- Internationalisation. The protection is granted, through international treaties, throughout almost the entire world. The standardisation of Authors' rights at the international level is at a very advanced stage.

Notwithstanding these advantages, the application of Authors' rights to software has not been easy. The standardisation of protection at international level, equating computer programs to literary works and their protection under the system of Authors' rights are complicated matters, applying provisions that were originally devised for quite different works. Additionally, the laws of the continental countries have incorporated in their Authors' rights systems

this solution for the protection of software that is ultimately conceived for the copyright system of Anglo-Saxon countries, giving rise to difficulties with the traditional characteristics of the continental system, especially the recognition of moral rights.

3. Authorship and works created in open collaboration

This section explains the various actors that may be involved in the process of creation and distribution of works and the various types of recognised authorship. Due to the numerous factors involved in the process of creation of software, and especially free software, this section is especially relevant.

3.1. Authors

The author is the individual or human person creating a work. In general, ownership of rights in the work corresponds to the author due to the mere fact of his/her own original creation, by the principle of automatism, without requiring any additional formality or registration.

The status and recognition as author of a work (a moral right) is inalienable; it cannot be transmitted between the living or *mortis causa*, and is not extinguished with the passing of time. It does not become a part of public domain and is not subject to any statute of limitation.

- **Multiple authors**

  Works, including in particular software, may be created through the effort and labour of a single person or may be the result of a combined effort of several. This second scenario is more and more common in practice and, in these cases the attribution of authorship may prove more complex. The legal framework has established various figures to deal with these situations, which are not completely satisfactory, and vary significantly between jurisdictions. The following provides a very general summary.

  - **Collaborative or joint works**. A collaborative or joint work (work of joint authorship, in the copyright tradition) is that which results from the collaboration of several authors to create a single work, often where the contributions may not be distinguished. In this case, rights correspond to all authors in the proportion that they determine. In the absence of agreement, the authors are equal-part owners. While legal systems vary, usually the dissemination and modification of the work requires the consent of all authors. Nonetheless, once the work has been disclosed, none of the co-authors may unjustly refuse their consent to its exploitation as disclosed. Co-authors may exploit their contributions separately (if separable), provided no damage is caused to the joint exploitation of the whole.

  - **Collective works**. A collective work is generally a work created at the initiative and under the coordination of an individual or legal person, who publishes and disseminates the work in his/her or its own name.

> **Example**
>
> Extreme programming, online wiki text contributed by several authors.

> **Example**
>
> Encyclopaedia, anthology, certain free software distributions such as Mozilla code.

It represents the gathering of the contributions of several authors, in such a manner that it would be impossible to attribute to any of them the right to the overall work and each contribution is merged into a single, autonomous creation. The result is work with value added to the mere aggregation of contributions.

The rights in the collective work are owned by the sponsor or "editor", who publishes the work, without prejudice to the rights of each contributor in his or her contribution. Copyright in each separate contribution to a collective work is distinct from copyright in the collective work as a whole, and vests initially in the author of the contribution.

The concept of collective work needs to be treated carefully, as there are variations on how the term is used among different legal traditions. E.g. within the US system it refers to a combination of previous works assembled into a collective whole, usually arranged in such a way that the resulting work as a whole constitutes an original work of authorship. This in certain European systems is called a "composed work" or "compilation"[1] (indeed, in the US this term is also used).

[1]One important difference seems to stem from whether there is an "editor" who coordinates the work, and whether contributions are expressly made for the collective work (commissioned), or merely combined by a person into a compilation (e.g. using software libraries).

These figures do not necessary cover all forms of collaboration, especially in the world of collaborative creation of free software as we comment below.

- **Employee works and works for hire**

   Another situation to consider is the creation of works within the context of a legal entity or organisation, by employees. In this case, the general rule – and the specific rule for software (EUCPD – Art. 2.3) – is that when an employee creates a work in the exercise of his or her assigned duties or following instructions from the employer, the ownership of the economic rights corresponding to the work corresponds exclusively to the employer, unless otherwise agreed.

   Note that the employee is still the author, but the economic rights in the work are presumed to be held by the employer.

   As regards works created on commission, or "work for hire" within the US tradition, the EU frameworks have chosen not to regulate the subject matter and it has been the case law that has established that, except as otherwise agreed, there shall be no automatic transmission or assignment of rights from the original author to the person who commissioned the work. The ownership is vested in the creator and not the person (individual or legal person) commissioning the work (the client). As an exception, if the client is involved in the creative process of the software, authorship may become joint or collective.

   Usually, for an employer to be considered the rightsholder in a computer program, two requirements must be met:

   - The labour relation must be materialised by an employment contract.

- The program must have been created by the employee in the exercise of their duties or following instructions from the employer.

Such legal assignment of the equity rights to the employer does not preclude the moral rights from continuing to be the inalienable property of the programmer, in continental systems.

- **Rightsholders and free software**

The particulars of the free software development models, where the contribution of several programmers to a single work is common, add difficulties to traditional authorship models. To determine who the author is, who has the rights to the work and thus who can determine the license and has the legitimate right to bring actions for infringement, it is necessary to determine the type of work created and its owners. The answer will depend on the specific development model used, the existence or not of a coordinator, the possibility of separating the various contributions or not and, clearly, the specific agreements reached.

In a collaborative or joint authorship model, for example, each author is the owner of their contribution and of the whole, the work being exploited collectively. This implies that if a development model of the software of this type were chosen, it would be essential for the authors to reach an agreement, as soon as possible, with respect to the licence that would be applied to the software (as a whole) and the system of exploitation for the resulting work. In collective works, where there is a coordinator, the rights and exploitation of the work as a whole should be clearer and it is the editor who may protect the rights in the collective whole (but not necessarily the contributions).

Example

Examples of free software applications that could be considered collective works (if developed and disseminated under the Authors' rights system) include the Mozilla programs, coordinated by Mozilla.org, or certain applications of the GNU project of the Free Software Foundation. There are also "business" applications, such as JBoss, Jasper Reports, OpenOffice.org, SugarCRM, Openbravo, etc.

To prevent possible future problems, the projects for the development of free software electing this option often ensure that each author-contributor licenses or assigns their rights in writing, exclusively or non exclusively, to the coordinating entity, so that it may correctly manage the intellectual property rights to the application, specifically, determine the licence system, guarantee the defence of any infraction, etc.

Example

An example of this preventive policy may be found in the conditions of the FSF for any contribution made by programmers providing more than ten lines of code for a project coordinated thereby: they must transfer ownership of the code to the FSF. A Fiduciary License Agreement has been drafted within the EU for this purpose. Other established projects (Mozilla, OpenOffice.org, Apache, Eclipse, etc.) require a license or assignment of rights of one type or another. See the sites of Apache Software Foundation and Eclipse.

3.2. Ownership of rights in a derivative work

As we have already studied, an original work is a work of autonomous and independent creation, even if published collectively with others. A derivative work, on the other hand, is a new work resulting from the transformation of pre-existing work, usually without the collaboration of the author of the latter, but with his/her permission (see below).

As the derivative work constitutes a new work, even if it is based on another, there are therefore two different works and two sets of rights: in the original work and the derivative work. We will see below that the author of the derivative work needs the permission of the original author or rightsholder in order to create this new work, and must exploit the new derivative work in accordance with the licence granted by the original rightsholder.

We will also see below that copyleft (in the GPL or other copyleft license) is a free software licensing mechanism enabling others to create works based on existing software, but forcing the new author, if he/she redistributes the new work, to do so under the terms of the same copyleft free software licence – i.e. maintaining the freedom of the work.

3.3. Identifying the author and/or rightsholder

As the original authors or rightsholders to a work are those that can first exploit or authorise the exploitation of a work, and may also assign the rights thereupon (by licence) to a new rightsholder, it is clearly important to know the methods of identifying the copyright holders.

The © symbol, intellectual property registration and authorship recognition notices in the work itself are the most common instruments for identifying the owner of the Authors' rights to any work, although such formalities have not been mandatory since the Berne Convention.

Generally speaking, copyright law provides that:

•   The author shall be presumed to be whoever appears as such in the work by name, signature or mark identifying them (notice of authorship: © Jane Smith, 2007).

•   If the work has been disseminated anonymously or under a pen name, the exercise of the rights shall correspond to the person disseminating the work with the consent of the author.

- The assignment of rights by the author, as a general rule, is not presumed: it requires a specific act in writing. In the absence of such act, the owner reserves all rights.

For free software, the identification of the author may be problematic, for instance, in the event that there are several anonymous authors contributing code to a particular application (Mozilla, GNOME, KDE, etc.). Such difficulty in identifying the author may cause problems when requesting consent for a change in licence or for active authentication in the event of an infraction.

To deal with this type of problem, the coordinators of certain free applications maintain lists of contributors and have established lists of unidentified authors. For instance, the Free Software Foundation requires that each contributor should identify themselves with the project coordinator. MySQL AB only accepts contributions to its free database engine from those that have signed its developer's agreement.

One requirement common to all free software licences is the compulsory mention of the ownership of the original work by maintaining the copyright notice. Nonetheless, each licence establishes different requirements in respect of the public notices of authorship (for instance, in the documentation).

> Along these lines, the Apache licence requires that the mention should be maintained in derivative works of the authorship of the original software, while the GPL requires providing indications that the work has been modified, when and by whom. The MPL requires indication or description of the changes (e.g. with a diff file).

4. Rights in protected works

In this section we will study the core of Authors' rights: the rights invested in the author or owner of the rights to the work. In the continental system, two types of rights are distinguished: personal or moral rights and patrimonial or economic rights.

4.1. Personal or moral rights

The continental system of Authors' rights supports the intimate connection between the author and the work and, as opposed to the copyright system, declares that authors have a "moral right to limit the modification and manifestation of their work", even after having transferred its economic rights to a third party. The moral right of authors to their work is made up of several rights and that, to simplify, serve to "protect their name and the integrity of the work" and prohibit any modification without their prior consent.

While national regimes vary, the following moral rights are generally granted to the creator:

• To decide in respect of the dissemination of the work.

• To determine how the dissemination is to be made, in their name, under a pen name or anonymously.

• To the recognition of their name and the respect for their status as authors.

• To demand that the integrity of their work be respected and to prevent any alteration thereof that could imply any damage to their legitimate interests or undermine their reputation.

• To modify the work, respecting the rights acquired by third parties and the requirements for the protection of goods of cultural interest.

• To withdraw the work from the market for changes in their intellectual or moral convictions, upon prior indemnification for damages to the owners of the exploitation rights (right to repentance).

• To access unique or rare copies of the work, when in hands of another, in order to exercise dissemination rights or any other of their vested rights.

These personal rights accompany the author during his/her entire life, being non-waivable, non-transferable, inalienable and some are even perpetual (i.e. inherited by heirs of the author).

When regulating Authors' rights applied to software, in the Computer Programs Directive of 1991 there is very limited mention to moral rights and there is no mention to the other equity rights of authors (compensation rights, as we shall discuss). Nonetheless, the majority of the doctrine understands that moral rights do apply to software.

The recognition of the moral rights granted under the continental system to the authors of computer programs may prove inconvenient for companies engaged in the manufacture of software (think of the repentance right). Doctrine sustains that a way to avoid them is to strip individuals of the authorship of programs. In the development of proprietary software, companies may take over all the rights as employers or as publishers or coordinators of a collective work.

In the development of free software, the matter is more complex. To determine the existence and the possible owners of moral rights, it is necessary to study the specific development model and the agreements reached by the various programmers involved in the creation.

What is interesting, however, is that nearly the ONLY requirement common to all free software licences is that of maintaining the original copyright notices, and for many licences that of identifying if a work has been changed. This is a documentary form (if not necessarily contractual) of respecting moral rights.

4.2. Economic or patrimonial rights

Economic or patrimonial rights are based on the conviction that authors should be compensated for exercising their unique creative abilities, thus promoting the creation and dissemination of new works. The law therefore grants certain exclusive rights to rightsholders enabling them to obtain pecuniary benefits derived from the work, through exclusive use or assignment or licensing to third parties. In exchange for the transfer of rights, the author shall receive compensation (or not), which is generally proportional to the income generated by the exploitation of such work.

In some jurisdictions, like Spain and France, these rights are conceptually divided into the rights to the exploitation of the work and rights that are merely compensatory in respect of others' use. These are discussed in further detail below.

Exclusive exploitation rights are those recognised by law to their owner and grant an exclusive power to exercise or authorise (and, accordingly, to prohibit) beforehand certain forms or acts of exploitation with respect to their work. Acts of exploitation include, without limitation, reproduction (copy), distribution, public communication and transformation.

EU Computer Programs Directive, Article 4

Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2, shall include the right to do or to authorise:

(a) The permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole. Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightholder.

(b) The translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program.

(c) Any form of distribution to the public, including the rental, of the original computer program or of copies thereof.

As may be seen, the exploitation rights of the author of a computer program are basically the same as those for any other work, although they must be adapted to its own characteristics.

4.2.1. Reproduction right

Reproduction consists of incorporating a work or any part thereof on a medium allowing for its communication and obtaining further copies, directly or indirectly, provisionally or permanently, by any means or in any form. Even short-lived copies are considered reproductions.

EUCD, Article 2. Reproduction right

Member States shall provide for 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...

Acts requiring authorisation

In principle, the following acts require authorisation, as they constitute reproductions:

- Downloading from the net and storage to a local hard drive or flash card.

- Making copies on CDs, DVDs, or flash memory (subject to the right to make private copies or fair use).

- Transmission: the delivery to another system by telecommunication, local network, etc. or uploading of files onto a web server, or their download to a local computer (for instance, P2P transfers) or attaching a file to an email and sending it.

- Loading a program to execute it: introducing the program into the RAM.

- Presentation: on-screen visualisation of the graphic interface.

- The integration or incorporation of the code lines of a third party in a new development.

> **Supplementary content**
>
> Note that the EUCPD does not apply the public communication right (e.g. transmissions in digital format via the web) to software, however it is generally understood (either by doctrine or case law) that software is subject to this exclusive right.

The right to copy or reproduce (except for backup or security copies and private copies, the former being permitted and the latter prohibited in relation to software, as we shall see) is fundamental in licences, as it is necessary to have it to be able to run/use the program. We should nonetheless note that a "legitimate user" (say a user with a "usage licence" that does not necessarily specify the relevant rights, as is the case with many poorly-drafted licences) does not require such authorisation merely to use the program (Article 100.1).

The subject of reproduction is quite controversial and difficult to resolve in relation to the software, due to the diverse nature of a program: it is made up of the elements of design (its architecture and structure), code lines (which may be object code or source code) and the result of its performance. A reproduction may take place at any level or in relation to any element.

A **verbatim reproduction** of the code lines without authorisation (cut and paste) is the most common infraction in relation to computer programs. However it is considered that there are other forms of reproduction, known as **non-verbatim reproduction**, which may also constitute breaches of the reproduction rights. Non-verbatim elements of a program can include its structure and architecture, data input and output formats, API format, graphic interface (look and feel), etc. Defining whether or not a copy exists in the case of two programs that are similar in non-verbatim elements is a complicated matter.

> **Examples of non-verbatim copies**
>
> An interesting element for study in relation to non-verbatim copies would be the case of two different programs that have similar results. It could be the result, for instance, of the re-engineering of the first (the creation of a new expression of the underlying ideas), which would generally be permitted by law, provided the result of the re-engineering were not done through studying and reviewing the code of the first software.
>
> Another scenario would be that in which, although no verbatim copy of the lines of the code of the original were used in the development of the second program, it could be argued that the second is a copy of the first due to the functions, structure, data organisation and/or the result of its process (the graphic interface, for instance) being –too– similar.

There is a certain amount of case law on non-verbatim copies of computer programs, especially in the United States, although unfortunately, for the time being, there is no final and unanimous answer to the question. In the United Kingdom, for instance, the test currently accepted by the courts is that a copy exists if, in the development of the second program, there has been use of the "*skill and judgement of the original authors*" in reference to the data structure, the system architecture, the development and implementation methods, the graphic interface, etc. Therefore, to defend from unauthorised copies, it is not always necessary to prove the existence of a verbatim copy (a task that is usually difficult due to the lack of access to the source code of the infringing program and its development documents).

These elements are especially relevant in the development of free software as several free applications imitate, and often improve on, proprietary applications. Additionally, proving the existence of copying is easier with the free software, as its source code is distributed openly.

4.2.2. Right to distribution

Distribution is understood as the making available to the public of the original or copies of the work by sale, rental, loan or any other means.

EUCD Art 4: Distribution right

EUCD Art 4: Distribution right. 1. Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.

This right covers for example the sale of books or magazines in shops, the distribution of software in boxes (via ecommerce or on the shelves of computer shops), or the distribution of works on CDs with magazines.

Distribution requires the use of tangible copy, therefore, in cyberspace the concept of distribution is distorted and, as we shall see, that of public communication is reclaiming its relevance.

One of the most complex issues in this matter is the **exhaustion of distribution rights**. This basically means that once a copy has been distributed, the rightsholder can no longer control the exploitation (sale, redistribution) of that copy.

The exclusive distribution right of the owner "is exhausted" with the "first sale in the European Union of a copy by the owner of the rights or with their consent", except as regards the rentals/leasing of the program (in this case, there is no exhaustion for distribution outside the EU). Facing this possibility, software suppliers are careful to clearly establish in their end user licence that they are not "selling" any copies to the user, as this would imply their waiver of the exclusive right to control the distribution of the copies and the user could freely distribute their copy (although they could not make any subsequent copies for distribution), at least in the European Union.

Accordingly, in most licences, the owner/supplier "sells" the software medium (the CD-ROM), but with respect to the software it solely grants the user the right to use it by licence, prohibiting their transmittance of the usage right.

Unauthorised software copies loans? There is certain discussion as to whether the owner of the exploitation rights may prevent certain users from "lending" the copy of the software. A loan is distinguished from rental in that, although in both cases the user temporarily assigns the copy to a third party, the loan is free of charge.

Example of Spain

In Spain, the law provides a general exception (for literary and artistic works, etc.) to the distribution right for certain cultural institutions of general interest (museums, libraries, etc.) who are allowed to make loans without having to obtain authorisation from the owners or pay them any compensation. It is understood that this exception does not

apply to software. Therefore, although we may believe that such prohibition is often excessive, under a strict interpretation of the law, libraries or teaching institutions cannot lend software without express authorisation.

4.2.3. Right of public communication

The concept of public communication is originally conceived for theatre, movies or traditional radio, i.e., for acts of public broadcast of a work without the distribution of hardcopies.

EUCD Art 3: Public Communication

Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

With the implementation of the 2001 EU Copyright in the Information Society Directive, public communication was extended from "*any act whereby a plurality of persons may access the work without the prior distribution of counterparts to each of them*" (except within a strictly-domestic environment), to "*making available to the public through wired or wireless procedures, so that anyone may access them from the place and time of their choice*", a term devised for the distribution of works over the internet.

Breach of the right to public communication

A practical example of the breach of this right is the uploading of a program onto the internet on a given site (Warez, for instance) or making it available to third parties from the computer itself, using P2P programs such as eDonkey, eMule, Kazaa, etc.

Two clarifications:

- This right does not encompass private communications and, therefore, it is not considered to be a public communication or making available when made within a strictly domestic environment, not integrated or connected to a broadcast network of any sort.

- There is no exhaustion (Article 3.3 of the Directive).

The problem is how to separate what are public communications from what are private communications on the internet. For instance, is there a private communication if we send a document to fifty friends? What if we set up a "private" peer to peer program and solely open our computer up to certain people?

4.2.4. Transformation right

The transformation of works includes their translation, adaptation and any other modification by which a different work is created. Should the transformation be made without authorisation (express or implicit through the collaboration of the author of the pre-existing work), the Authors' rights of the rightsholder of the original work shall have been violated.

As we have already noted, the Authors' rights or copyrights in the work resulting from a transformation correspond to the new author. This author will nonetheless require authorisation from the author of the pre-existing work during the entire term of protection of their rights to the original work, to exploit the results by any means (e.g. directly or by distribution to third parties) and, especially, through its reproduction, distribution, public communication or new transformation.

There are certain limits to this right in relation to software, as we will see below.

Transformation rights and free software

As we have explained in the section on original works and derivative works, the model commonly used for the development of free software often implies the transformation of pre-existing works.

Therefore, free software licences consider the licensing of such transformation right one of the bases of software freedom. In other words, if a licence does not grant any transformation rights, it is not a free licence.

While there is significant debate about the scope of a derivative work, it generally results from a modification of the original work (adding, eliminating or modifying elements from the prior work) and/or, more arguably, its integration into a greater work that is based on the component (however, this depends on its form of integration).

> **Binary software**
>
> For example, binary software is defined as a transformation of the source code, and an implementation of the code for other hardware/devices.

Derivative works require the authorisation of the rightsholder in the prior work (express via licence, or implicit through the collaboration of the author), and a work incorporating pre-existing work without authorisation would infringe upon the Authors' rights of the owner of the original work, as we will see below.

Derivative works are a controversial subject with respect to free software, due to the difficulties in distinguishing between derivative work, collaborative or joint work and collective or composed work and what authorisations are required to create a work including third party components, libraries, etc. The difficulties arise basically in two respects:

- In relation to the **process of creation** of free software, this distinction is quite relevant for, as we have seen, free software is based on the incorporation, adding and modification of pre-existing work. The usual free software development model implies a substantial amount of contributors to the same application. Some authors provide new code (thus creating collaborative or collective works); others correct or improve an existing code (thus creating derivative work). Some authors also add a notice of authorship, while others do not.

  A key to the prevention of authorship conflicts in a free software development project may lie in the "*contributive intent*" of each author and in the proper management of intellectual property:

  – In the absence of an express agreement in terms of the conditions for collaboration, those managing software must rely on an implicit assignment of rights (which is not legally valid) or on the absence of claims by the contributing programmers facing any form of exploitation.

  – Good management of the process of collaborative creation requires an assignment or express license of rights by a specific agreement, such as a contribution agreement, or through the requirement that contributions should be made under a "project licence" or a compatible licence.

- Regarding the **use and exploitation of free software**, this distinction between original and derivative work is also important. All free software licences allow for the modification (adaptation, translation, etc.) of applications and, therefore, the creation of derivative works. Some free software licences impose conditions on the redistribution and use of such derivative works (the GPL for instance), while others do not (the BSD).

It is thus important to properly understand the definition of derivative work to know whether a development made based on a free application (for instance, integrating it, modifying it, using it, etc.) may be considered work that is derived from the original (and, therefore, to have respected the conditions of the licence with regard to modification and redistribution) or an original work using it without modifying it (an independent work, with its own licence).

4.2.5. Strictly-compensatory rights

Strictly-compensatory rights are basically the right to participate in the resale price of plastic works (*droit de suite*) and the right to compensation for private copies. The right to compensation for private copies is held to be an inalienable right of the authors and artists, interpreters or performers, compensating the intellectual property rights not received for the reproduction of the protected works or services to be used exclusively privately by the copyist.

The levy on blank CDs

It is important to know the impact that the right to compensation for private copies due to the consequences that the application of a levy to virgin CDs will have for users of computer programs. In Spain, for example, the levy has been imposed to compensate the private copies of music that may be made by private persons. But the same CDs are

used to make security or backup copies of computer programs, leading to the argument that this solution is unfair, and the courts have on several occasions required the levy to be returned.

These levies are managed by collecting societies, bodies like the PPL in the UK, SACEM in France, or SGAE in Spain, which we comment on below.

4.3. Other rights protected

The legal framework also restricts certain "secondary" acts, in the sense that they are not direct breaches of exclusive rights, but indirectly affect them, associated with software, and may constitute intellectual property violations:

- Putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy (this could arguably be extended, for instance, to companies basing their business on distributing P2P software expressly stating its use for sharing music files).

- The possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy.

- Putting into circulation, or the possession for commercial purposes of, any "*means*" the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device (a Technical Protection Measure, or TPM) which may have been applied to protect a computer program (e.g. rippers and cracks).

In certain circumstances, the general regime of copyright law also punishes those who aid and abet the commission of a breach (e.g. by providing services of transmission, broadcasting or distribution of illegal works with knowledge); and the manufacture, marketing or distribution of articles destined for the illegal copying of protected works.

Supplementary content
Any infringing copy of a computer program and any illegal means for eluding technical protection mechanisms (TPM) shall be liable to seizure in accordance with the legislation of the Member State concerned.

5. Limits of authors' rights/copyright – fair use

As we have seen, the author or rightsholder of a work has virtually absolute control over its use. Nonetheless, general interest imposes temporal and substantive limits on such monopoly of the author or rightsholder, recognised in the legislation on Authors' rights. Set out next are the exceptions or limitations recognised by law with respect to the rights that we have seen in the preceding section.

5.1. Time limitations: duration

Ownership is eternal; nonetheless, intellectual property is subject to a term. Throughout the entire European Union, the general rule applies that after seventy years have lapsed from the death of the author or the declaration of their death, the work becomes part of the public domain. Works in the public domain may be used by anyone, provided their authorship and integrity are respected.

Notwithstanding the general seventy-year rule, there are special terms for certain types of work. For instance:

- Exploitation rights for anonymous or pseudonymous works shall endure seventy years from their lawful dissemination.

- Exploitation rights for collaborative works shall endure the entire lives of the co-authors, plus seventy years from the death of the last surviving co-author.

- Exploitation rights to collective works endure seventy years from the lawful disclosure of the protected works.

- The rights to "business" works endure seventy years from the 1st of January immediately following their first publication.

Authors' rights in the United States

The duration of Authors' rights in the United States is complex, as it is dependent on various factors, including whether or not the work has been published. The general rule for works created after 1 January 1978, is that they are protected by intellectual property rights during the life of the author, plus an additional seventy years. For anonymous, pseudonymous or commissioned works, copyrights last ninety-five years from their first publication, or one hundred and twenty years from their creation, whichever term expires first. For computer programs, the duration of copyright in the United States is fifty years after the death of the author or seventy-five years from the publication of commissioned works.

It is also necessary to bear in mind that neighbouring rights have shorter terms and that moral rights, such as paternity and integrity, are perpetual.

5.2. Substantive limits: exceptions

As we have seen, exploitation rights are not absolute, inasmuch as the law specifies, as exceptions, certain acts which may be performed without express authorisation and sometimes even without compensation.

The purpose of the exceptions in most works is to protect the public interest, such as education, access to culture, freedom of information and criticism, and free competition. All limitations must be applied in accordance with the Berne three-step test, i.e. in certain specified cases which do not conflict with a normal exploitation of the work and which do not unreasonably prejudice the legitimate interests of the rightsholder.

This is not the place to enter into a long discussion on the exceptions, much of which took place during the drafting of the EUCD, however we find it of use to present the (summary) list below. The list seems long, however they are often limited in manners which make their use difficult (e.g. public education – what about private or charity-based education?).

EUCD Article 5 – Exceptions and limitations (summary)

- Temporary acts of reproduction .... which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use...

- Reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation...

- Reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation...

- Specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage...

- Ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives...

- Reproductions of broadcasts made by social institutions pursuing non-commercial purposes...

- Illustration for teaching or scientific research, as long as the source, including the author's name, is indicated...

- Uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature...

- Reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics... in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated.. or reporting of current events, to the extent justified by the informatory purpose...

- Quotations for purposes such as criticism or review, ...

- Public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings...

- Political speeches as well as extracts of public lectures or similar works...

- During religious celebrations or official celebrations organised by a public authority...

- Use of works, such as works of architecture or sculpture, made to be located permanently in public places...

- For the purpose of caricature, parody or pastiche...

- In connection with the demonstration or repair of equipment...

- Communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of [public libraries, education] establishments...

- Other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community...

We note that many of these limitations are qualified by "*to the extent justified by*" the purpose in question and "*use is in accordance with fair practice, and to the extent required by the specific purpose*", and often provided compensation is given to the rightsholder.

Exceptions in relation to computer programs

The above list does not apply to computer programs, whose exceptions are set out in the 1991 EU Computer Programs Directive.

The purpose of software copyright exceptions is to ensure that the legitimate user of software (who has validly acquired a licence) may use it in accordance with its purported use. Otherwise, the right of use would be deemed distorted and to not correspond with what could legitimately be expected by the user. In non-free software licences, the owner of the exploitation rights to the program grants few rights. Exceptions therefore play a key role, although the absolute exclusion of the use of the program has no exception with respect to who is not a "legitimate user" of such program.

The Authors' rights system has elected to establish a closed system with a specific list of exceptions. Exceptions to Authors' rights applicable to software are developed in Article 5 EUCD and may be summarised as the authorisation of the **legitimate user** to:

- Reproduce and transform the program when necessary for its use, including debugging (limitable by contract).

- Making a security or back-up copy (absolute right).

> **Supplementary content**
>
> In free software licences, the granting of exploitation rights is so broad that it breaks the monopoly of the author and often makes such exceptions irrelevant.

- Analysis of the program to determine the ideas and principles on which it is based, while loading and running the program.

- Reproduce and transform certain necessary parts of a program to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, on certain conditions.

This last is considered a reverse engineering or quasi decompilation right, however it may not be exercised if the owner of the program has provided the relevant information.

A "legitimate user", while not defined, is understood to mean a person with a "use right", such as under and EULA or other form of software licence.

<table>
<tr><td>**Supplementary content**</td></tr>
<tr><td>In contrast, the copyright system contains an open clause for fair use, allowing a certain margin to the judges for each specific case. This subject shall be explained further ahead, in the section on copyright.</td></tr>
</table>

Acts of reverse engineering

Reverse engineering may be defined as all operations necessary to determine the ideas underlying the computer program. It is not limited to decompiling. The establishment of an authorisation to perform acts of reverse engineering is intended to guarantee the development of a non-monopolistic industry and interoperability, and at the same time to battle against the reverse engineering that is intended to discover the source code through the object code. This includes therefore the rights of:

- Analysis during normal use.

- Decompilation for interoperability, subject to the following conditions:
  - Only the legitimate user or anyone authorised to use the computer program, or a person duly authorised in their name (such as the company), may perform acts of decompiling.

  - The owner of exploitation rights has not made a version of the source code (at least the part that can allow interoperability) or interface information readily available.

  - The decompiling must be limited to the parts of the program that are necessary to achieve interoperability.

Once the information is lawfully obtained, restrictions are established on its use:

- The information cannot be used for purposes other than those of acquiring interoperability for a computer program created independently.

- It cannot be communicated to third parties, except as necessary to achieve the interoperability of the program created independently. Along these lines, the person that has decompiled a program has a legal obligation to confidentiality.

- It cannot be used for the development, production or marketing of a program that is substantially similar in its expression or any other act infringing upon the Authors' rights.

Finally, a general limitation exists that indicates that the provisions relating to decompiling cannot be construed in a manner such that their application causes "unjust damage to the legitimate interests of the owner of the rights or is contrary to the normal exploitation of the computer program". This limitation, seemingly theoretical, has some practical application: when the decompiling operations to obtain interoperability with other programs may damage the rights and expectations of the owner of exploitation rights (exclusively marketing software, issuing new releases, etc.), the user must also refrain from performing them, which implies that this right of the user may be impracticable.

5.3. Fair use

In the United States copyright system, one of the most important limitations is the "fair use" doctrine. The referred doctrine provides that the exclusive rights granted to the owner of the Authors' rights do not include the right to prevent others from fairly using the registered work. The doctrine has been developed based on a substantial number of judicial decisions over the years and has been coded in section 107 of the current Copyright Act. This contains a list of the various purposes for which it may be considered "fair to reproduce any work in particular, such as for purposes of critique, commentary, news, information, teaching, academic studies or research".

Section 107 US Copyright Act

Section 107 US Copyright Act establishes four factors that must be considered to determine whether a particular use is fair or not and, therefore, if it is excluded from copyright violation:

1) The purpose and nature of the use, including whether it is commercial in nature or has educational, non-profit purposes.

2) The nature of the work protected by Authors' rights.

3) The amount and degree in which the portion used is important in relation to the overall work protected by Authors' rights.

4) The effect of such use on the potential market or the value of the work protected by Authors' rights.

A significant amount of case law has developed this concept and applied it to a variety of cases, including in relation to software.

6. Copyright

Now that we have seen the basic tenets of Authors' rights, which are also those of copyright, we can comment briefly on the differences between the two protection regimes.

- The object. The copyright system revolves around the work and the benefit that it provides to the common interest. The authors and their rights therefore assume a secondary role, as opposed to the tradition of Authors' rights.

- The absence of formalities. Traditionally, the copyright system established certain formalities for works to be protected, specifically their registration, and it was not until the Berne Convention that such requirements were eliminated. The copyright system currently is completely devoid of formalities and procedural requirements, similar to the system of Authors' rights. The United States nonetheless continues to demand that its own citizens, but not foreign authors, register their works at the Copyrights Office to be able to defend themselves at the federal courts.

- Low level of originality. The threshold of originality (novelty, creativity) required for works to be protected by the copyright system is quite low: it is solely required that the work should be new and should have been created by its author, i.e., that it should not be a copy.

- Moral rights. The copyright system does not recognise the existence of moral rights in computer programs, and therefore allows the complete transfer of the Authors' rights to an application or a code line to a third party.

- Duration. In the copyright system, the duration of protection of the works is generally longer. In the United States, for instance, duration is a complex issue, which may be seventy, ninety-five or one hundred and twenty-five years. In the United Kingdom, as the matter has been harmonised at a European level, its duration is the same as in Spain: generally seventy years from the death of the author.

- Authorship systems. In the copyright system, when there are several authors, and their contributions cannot be distinguished (which is equivalent to collective works), authors are considered co-owners under a joint-ownership system. There is nonetheless no concept of collaborative work when the contributions to works may be distinguished from one another, and in such cases, we would be dealing with a mere compilation of

individual works. If the compilation is original in any way, it is deemed collective work.

- Permitted acts. In addition to the aforementioned limits to the exclusive rights of software owners, copyright provides a "fair use" defence that we have commented on above.

- Transmission or transfer of rights. The copyright system allows several means of transmission of rights to protected works:
  - Full and exclusive assignment: contrary to that established in continental law, the copyright system allows the transfer of all the rights of the owner of a work. The assignment must be made in writing and be signed by the assignor. The assignee shall have all rights to the work, without restriction.

  - Additionally, the assignment of future works (although not "all" future works) is possible (for instance, under a service agreement between a client and an autonomous programmer): upon creation, the ownership of the work shall be vested automatically in the client.

  - Licence: the most common means of transmission of rights.

  - Work for hire: an automatic assignment of rights applies in favour of the person commissioning a third party for the development, as opposed to the Spanish system. The agreement must indicate that the commission is of such nature.

- Databases. To date, in the United States legislation similar to the European for the protection of databases has been rejected due to the pressure by the scientific and educational community, which claim that protection such as that granted in Europe would prevent free access to information. Nonetheless, the effort (sweat) devoted to databases is protected, without the formality of the European regime.

7. Database / *Sui Generis* Rights

To obtain a broader vision of all aspects of Authors' rights relating to software, we believe it is convenient to briefly address the legal protection of databases. **Directive 96/9/CE by the European Parliament and the Council, regarding the legal protection of databases**, regulates the matter within Europe.

To understand the various protections existing, it is necessary to take into account that databases may or may not be considered original works.

7.1. Databases deemed original works

The basis for the protection of databases lies in the right of the author to protect not only absolute originality, but also derivative originality, i.e., creation based on other creations. Intellectual property and originality may be in the selection of content and its layout.

Therefore, a database may be considered original work and be subject to Authors' rights (assignment IP, which we studied above). In this case, the structure (choice and arrangement) expressing the creativity of the author in the database is protected, not its content.

7.2. Databases that are not original

Is there any originality in a list of telephone numbers or of associates in an organisation? Hardly. Not if the selection is based on criteria of comprehensiveness and arrangement is based on functional criteria (alphabetic or chronological order, for instance). This does not mean that such databases, created with great effort, should not be protected, but it seems clear that it should not be through Authors' rights.

Protection may be provided by unfair competition regulations or the granting of exclusive rights, arguing that the risk of copy is too high and that it is necessary to have the rights to exploit such databases. We should note that unfair competition law does not protect the acts of private parties with no commercial purpose or of non-rival companies. Below we shall see that the *sui generis* rights to databases and intellectual property are not affected by such limitation.

***Sui generis* rights to databases**

The option of creating a special, *sui generis* right in favour of the "manufacturers" of databases is embraced by Directive 96/9/CE, regarding the legal protection of databases.

> To date, legislation similar to the European for the protection of databases has been rejected in the United States due to the pressure by the scientific and educational communities, which claim that protection such as that granted in Europe would prevent free access to information. Europe defends the *sui generis* right to databases at the WIPO through an international treaty, which has nonetheless been faced by opposition from the United States and the developing countries.

This specific regulatory framework has the following characteristics:

- Object of protection. The *sui generis* right does not protect creativity, but a **substantial investment**, whether it be economic or in effort, made by the manufacturer of a database.

- Rights and infractions. The manufacturer of the database is attributed what is known as a *sui generis* right, consisting of the power to prohibit:
  - The extraction and/or the reuse of all or a substantial part, evaluated quantitatively and qualitatively, of the content of such database.

  - The repeated or systematic extraction and/or reuse of non substantial parts of the content, representing acts contrary to the normal exploitation of the aforementioned database or causing unjust damage to the legitimate interests of the manufacturer.

- Duration. In appearance, we are dealing with a short-term right (fifteen years from the completion of the database), although considering the legal framework, any substantial new investment would open a new fifteen-year term.

8. Collective management organisations and digital levies

We have seen that authors are granted exclusive rights in their works. These rights enable them to market the work, by assignment or licence, to third parties, in exchange for remuneration. This commercialisation and regulation of the use of works needs to be managed, and this can be done either individually or collectively.

When rightsholders manage the rights themselves, they license the works to commercial users such as publishers or producers or such as distributors. This is usually done by way of contractual licence (exclusive or non-exclusive), which may authorise a type of use only or all uses. However, due to the number of uses and users as well as rightholders involved, licensing certain rights individually has been impractical, particularly rights of remuneration.

The following is just a very brief overview of a complicated and controversial topic, which we only summarise as collective management does not apply to software, our main theme in this work.

8.1. Collective management

Collective rights management is the system under which a "collecting society" jointly administers rights and monitors, collects and distributes the payment of royalties on behalf of rightsholders. This system is used in particular to manage remuneration rights, such as compensation for private copies, and commercial use of works entrusted to the societies (broadcasting, public performance, use in bars and hotels, etc.).

> While the collective management of rights is not at all harmonised at international level (though most national legislation provides for some form or other of collective management), the system is touched upon in international treaties. E.g.: the Berne Convention states that Member States may determine the conditions under which certain rights may be exercised and managed through collecting societies. Directive 92/100/EEC, when harmonising the right to equitable remuneration, provides for collective management as a model for its management in Article 4. Under Article 9 of the Directive 93/83/EEC collective management is obligatory for cable redistribution rights.

At national level, significant differences exist with respect to both legislation and practice, and the framework is in constant development. Several legislatures (e.g. Spain) require mandatory collective management, i.e. such rights may only be administered by collecting societies.

With the advent of the digital environment, there is more and more cross-border trade in goods and services based on copyright and related rights, notably for the rights of reproduction and communication to the public and the mak-

---

Supplementary content

In France, Belgium, the Netherlands, Luxemburg and Portugal, for instance, new legislation has been adopted or initiated with the aim of rendering rights management by collecting societies more transparent and of improving their accountability.

ing available right. This has led to self-organisation of collective societies with an international framework (e.g. *International Federation of the Phonographic Industry, Business Software Alliance).*

8.2. Collecting Societies

From the rightsholders point of view, collecting societies are agents to manage the licensing of their works. From the users' point of view, they are a single point of contact when seeking a licence to exploit a variety of works (audio-visual, etc.).

Collecting societies usually administer, monitor, collect and distribute the payment of royalties for an entire group of rightholders, on the basis of the national law of its territory, with respect to that territory. They enter into agreements with other collecting societies at an international level for the mutual payment of levies to artists represented by foreign societies (cross-licensing).

Collecting societies manage rights in relation to music, literary and dramatic works as well as audiovisual works, productions and performances. The rights that are managed cover a variety of acts that a user may wish to exercise, such as mechanical reproduction and reprography (e.g. printing to a CD), communication to the public in general (shops, gyms, bars, hotels, terrestrial TV), cable retransmission of broadcasting programmes (cable TV, internet broadcasting), public lending, artist's resale rights, private copying or certain educational uses.

- From a rightsholders point of view, often only one society operates for each group of rightholders in the territory in question (authors, performing artists, directors and producers) and it is the sole access in the market to purchase a licence to use the works. In other countries, they may be represented by competing societies (e.g. Spain).

- From the users' viewpoint, collecting societies are a one-stop shop, representing a wide, if not worldwide repertoire and have an exclusive mandate for the administration of rights in relation to their field of activity. They enable the licensing of a variety of rights and providing access to a global portfolio of works.

A number of models exist for establishing a collecting society, which may be corporate, charitable, for profit or not for profit entities. They may also be mandatory (Spain) or recommended (UK). In exchange, collecting societies may be subject to control by public authorities or specific bodies, covering the behaviour of the societies, their functioning, the control of tariffs and licensing conditions and also the dispute settlement. With respect to the licensing

conditions, in some Member States the obligation of collecting societies to grant licences is combined with the rule that such licences should be granted under appropriate or reasonable conditions.

8.3. Criticism

There is broad criticism of the collective management system.

- Criticism from users is aimed at the tariffs and the inefficient supervision of collecting societies and access to the courts or arbitration to protect users' rights. It has also focussed on administrative fees charged by the societies, the length and difficulty of negotiations with respect to licences, alleged deficiencies in their internal decision-making process and an apparent lack of transparency regarding the pricing policy.

- Rightholders are also complaining. Those with a certain degree of bargaining power, such as major record and film producers, increasingly seek not to depend on collecting societies to manage their rights, and directly license their rights to third parties. This has been enabled by technology, with watermarking, rights information identification and tracking of the use of works, potentially enabling powerful companies to control the royalty payment process. Smaller rightsholders complain that the distribution of levies is not transparent. All in all, rightholders would like collecting societies to be more flexible in respect of the membership contracts (acquisition of rights) and for themselves to have more influence in the distribution of royalties.

> **Supplementary content**
>
> The levy on blank hard disks, CDs and DVDs is specifically seen as unfair, as these items are often used to copy private photos or enterprise's own software, which is not subject to remuneration right.

8.4. Collective management and software

There is no collective management of rights in software products, and no collecting society for developers. Privately, the Business Software Alliance represents the major private software manufacturers such as Microsoft, Adobe, etc. and engages in the monitoring and private policing of use of their products.

9. Legal protection of authors' rights/copyright

The information society, with digitisation and instant transmission of works over public and private networks, has set the scenario for greater access to information, culture and knowledge. But it has also led to greater levels of infringement of Authors' rights/copyright. In particular, use of software by someone other than its owner, without their express permission, is a use that is prohibited by the law itself.

When Authors' rights were conceived as a means of protecting works and, even currently, in the world of distribution on paper format, publishing houses and Authors' rights had a function, as authors needed their infrastructure to broadcast their works and copies were virtually nonexistent or were limited to the private scope of the copyist.

Over the years, the technological evolution has broadened these horizons and other types of works, languages and means of exploitation have appeared, requiring the adaptation of Authors' rights. Nonetheless, the information society and the new technologies have caused a radical change by making the traditional works (text, music, photographs, etc.) available to all, using a new medium, and by training everyone to become a publisher and distribute works without the need for middlemen, in great part thanks to the internet.

That same technological revolution implies that the capacity to copy and reproduce, for profit or otherwise, has become generalised. A few years ago, a CD recorder was only available at a recording studio, but today we almost all have one at home, on our personal computer. Not to speak of peer-to-peer systems for sharing files.

Therefore, the system of distribution of works and the elements upon which the authors and middlemen base their profits has been questioned. This has implied an irreversible change, in the face of which all intellectual property legislation must be redefined to return the balance to the parties at conflict.

The owners of the affected exploitation rights (mainly the music, movies and software industry) seek to use Authors' rights, no longer as a weapon of one business against another, as they were originally devised, but as a defence by a business/owner against the public violating their rights.

P2P

A case of particular interest is P2P file-sharing. It is a common perception that it is lawful to copy a CD to another CD or flash card/hard disk, or to convert a song from CD into MP3 format, and in particular to share them with third parties on P2P file sharing systems. In fact, these actions are often in breach of copyright, and, at least in theory,

Supplementary content

Purchasing a music CD from a street vendor, downloading software from the internet or installing computer programs without paying for licences are examples of practices that may infringe upon the intellectual property rights of others.

[2]See on ACTA, the EU site at European Commission Trade as well as Prof. Michael Geist's blog at Michael Geist blog (Michael Geist blog)

give grounds for civil action. Depending on the jurisdiction, certain defences may be available, in particular that of private copy.

P2P software and networks are themselves perfectly legal, as they have legitimate functions for sharing works among users – works that may have no copyright protection, works under free software or content licences, etc. What is not so clear is the sharing of protected works on these networks, especially as regards the public communication right.

In the middle of this debate is the position of the ISPs in relation to P2P networks or other sharing mechanisms (rapidshare, etc.), who – for the moment – do not police or monitor the activity and data that is being transmitted in their networks. They have access to the names and addresses (including IP addresses) of file-sharers, and are the target of the content and software industry either for providing evidence as to who is responsible for illegal online activity, but also as private "policemen", warning and shutting down network access when they have sufficient evidence of such illegal activity. This is the aim of ACTA[2] (Anti-Counterfeiting Trade Agreement), a proposed international treaty to reinforce the protection of IPR on the net, and oblige ISPs to take this role.

This position is awkward for ISPs as regards the privacy of internet users, their rights of access to the network (not yet considered a universal right, but getting there) and imposing on them quasi-judicial obligations as to policing the network.

In this section, therefore, we look at the means and measures provided to defend copyright holders' rights against abuse: the legal measures of protection for works and the reactions in possible infractions of Authors' rights. To clarify the subject, we will divide them into preventive measures (legal and technological) and reactive measures or solutions to infractions to copyrights. We shall also briefly reference criminal and administrative legislation.

9.1. Legal measures of protection

We refer here to the – preventive – mechanisms that the law recognises to protect the rights of the owners of Authors' rights. As we have studied, in countries party to the Berne Convention and the TRIPS Agreement, copyright protection does not require any formality. There are nonetheless formalities or mechanisms that, although not mandatory, are often convenient to prevent the infringement of Authors' rights or for subsequent use as evidence of authorship.

- **Registration of intellectual property**
  Although the registration of the work is not mandatory, in most countries it is a quite direct and economical procedure, granting important additional benefits as regards the burden of proof of authorship and date of creation (or at least, registration). In Spain, for instance, registration generates a legal presumption whereby those appearing as authors of a registered work are to be deemed by the courts to be its authors, unless proved otherwise.

  Some countries, such as the United States, may require that their own citizens, but not foreign authors, register their works at the Copyright Office (for instance, to bring a claim before the federal courts). In some countries, a registration of Authors' rights also represents prima facie evidence of the validity and ownership of Authors' rights.

- **Notarisation**
  As an alternative or complementary option to registration with the Intellectual Property Registry, it is sometimes advisable to have the complete

source code notarised in magnetic medium (CD, DVD) containing the object code, the user's manual, design of screens, analysis, preparatory documentation and other elements identifying the program, which may be of vital importance when offering expert evidence.

Notarisation may provide official evidence in a trial on the date of creation or deposit of a work. It has also been seen as a system that is more appropriate than registration, as it is more confidential and faster, involving less bureaucracy and providing a better description of the program.

- **The use of the © symbol or indication of reserved rights**
  By application of the Berne Convention, in most countries, a notice is no longer required for the work to be protected by Authors' rights. Nonetheless, it is common to use symbols or notices to warn users that the information is protected. The proper form of such notice is as follows: "[copyright [date] by [author/owner]". The © symbol is sometimes used as a reference to the copyright system.

9.2. Digital Rights Management

The aforementioned digitalisation and advances in new technologies not only pose risks for the owners of intellectual property rights, but also make it easier to manage and control acts of exploitation through access, identification and copy prevention systems. Thus on top of these fairly weak measures for protecting a work, the larger content owners (including both software and audiovisual industries) have started to rely on technology to do so: the implementation of **technological protection measures** (TPM), as part of "Digital Rights Management" systems (DRM).

These new systems for the management of intellectual property rights are supposed to revolutionise the relations between users and owners of exploitation rights to musical works, audiovisual works and software, mainly.

DRMS are technological processes for the management of Authors' rights allowing a certain control by the owner over their work. They are used to identify the works and their owners, to request prior consent from the owners by users or to make micropayments for à la carte services, among other functions. DRM systems can be used to clear rights, to secure payment, to trace behaviour and to enforce rights.

Below we shall discuss the main technological measures of protection of works and their legal treatment.

Supplementary content

These management systems clearly also carry implications for the free software community. A very current example lies in a free student program on DVD that could allow the capturing of the original data for copy onto the hard drive.

9.2.1. Technological Protection Measures

Various technologies and methods have been invented to protect works, including computer programs and the associated computerised objects (databases, etc.).

From a legal viewpoint, measure of protection may be defined as "*any device or medium destined for preventing or restricting copies of a work or reducing the quality of any copies made*".

Protection measures

Some examples that are already found on the market are:

- Access codes: often, to install a program, a unique identification key is required. Additionally, to access databases, especially online, it is usually necessary to introduce a user name and code (password).

- Unique identification systems: watermarks.

- Ciphering and encryption of works.

- Copy protection systems: measures to prevent the copying of digital works (for instance, the CSS system for DVDs).

- The systems used by Adobe in its e-books, preventing printing or copying. Currently, to face the proliferation of technologies and groups seeking to avoid or break such devices (DeCSS, for instance), the law covers technological measures for the protection of intellectual property rights, as we shall see hereafter.

Using these mechanisms, a rightsholder can control the access and use of a work: technology can substitute and even exceed the law in the protection of the works. "Exceed" the law as this technology can also deny legitimate users and individuals the exercise of the rights under the exceptions provided by copyright law.

But TPMs, to be lawful and truly useful, also requires the protection and recognition of the right. To face this situation, one of the key reasons of the WIPO Copyright Treaty (WCT) in 1996 is the legal protection (against elusion, or cracking) of TPMs.

The WCT Treaty requires that countries subscribing to it should modify their legislations to provide two types of legal protection of technological measures:

- The first requires that the countries should provide appropriate legal protection and effective resources against the elusion of the technological measures used by owners to protect their rights.

- The second requires that the countries should prohibit the modification or deliberate suppression of electronic information regarding the management of rights, i.e., the information accompanying any protected materi-

al and that permits identifying the work, its author, interpreting artist or performer or owner, and the conditions for its use.

The WCT Treaty has been implemented in the Software and Copyrights Directives and now national laws. The legal framework in which DRM systems are administered is set out in the EUCD (Directive 2001/29/EC). Articles 6 and 7 deal with the protection of technological measures and rights management information respectively.

9.2.2. Legislation

Section 1201 of the Digital Millennium Copyright Act (DMCA) of 1998 in the United States and, later, Articles 6 and 7 of the European Authors' rights Directive in the Information Society have elected to make legitimate and offer legal protection to the DRMS systems by prohibiting devices and practices that allow for their elusion (deactivation, cracking, whatever).

This is a controversial subject as the result of the legal protection of these technological measures may be abusive if the owners of exploitation rights may completely control the use of the content rather than only intellectual property rights. Additionally, the technological measures protected by law not only increase the capacity of control of the owner of the rights to the work, without limitations, but may also affect the rights of the users as regards the interoperability capacity of the computer programs or private copy or educational use.

9.3. Measures of defence against the infringement of rights

Once the preceding preventive measures have proven unsuccessful and the Authors' rights to a work have been infringed upon, what we refer to as "measures of defence" come into play. Facing these infringements of Authors' rights, the legislation of both Spain and most of the states signing the international treaties offer a series of mechanisms for the protection of intellectual property rights, with the possibility existing of appealing to administrative, civil and criminal actions.

In the EU, national legislation usually provides civil protection of intellectual property, based on the idea of the repairing of a private right, rather than articulating an exclusive protection under criminal law, although this protection is notwithstanding any other action corresponding to the owner. Pressure from industry has widened actions to the criminal jurisdiction, as we shall see next.

Generally speaking, the national laws of EU Member States regulate the infringement of the rights in copyright protected works and action must be taken in national courts against copyright infringement: claim for breach of copyright, damages and interest. A rightsholder who wins this claim may request

seizure and destruction of the infringing work, and damages on the basis of earnings lost due to the illegal activity (often seen as a % royalty on the income of the infringing party).

In addition, the 2004 Enforcement Directive has increased and harmonised the measures at the disposal of rightsholders.

Note

The Directive is interesting because it also provides that Members States can be sanctioned by the European Court of Justice if their civil procedures on the infringement of intellectual property rights are "unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays".

The Enforcement Directive, now implemented in the EU jurisdictions, basically provides for the following:

• All Member States must apply effective, dissuasive and proportionate remedies and penalties against those engaged in counterfeiting and piracy.

• The collecting and preservation of evidence of breach: rightsholders can ask – both at trial but also as a preliminary measure, and without the defendant being present – for evidence regarding infringements to be collected, preserved and provided in court, including, if on a large scale, financial and bank documentation.

• At the request of a rightsholder, the courts may issue an interlocutory injunction (prohibition or order to do something) against the alleged infringer and relevant intermediaries, to prevent an "imminent infringement" of IPR or to prevent a continuing infringement, with penalty payments. This includes seizure of goods, freezing of bank accounts and other assets.

• Once a decision on the merits of the case has been obtained (inter partes, i.e. with the alleged infringer having presented his/her defence), the court can order destruction of the infringing products, recall and removal from commercial channels, and prohibition regarding future conduct, damages and costs.

• These rights can be exercised by rightsholders, collective management societies, and "professional defence bodies which are regularly recognised as having a right to represent holders of intellectual property rights" (e.g. BSA).

This directive was hotly debated during its drafting, due to a variety of reasons, not the least because many of the measures were deemed exorbitant and it sought to impose obligations on intermediaries to cooperate with authorities for providing evidence (e.g. evidence of online uploads and downloads of protected works).

9.4. Additional measures in relation to software

In relation to computer programs in particular, the EUCPD establishes certain specific acts that without the authorisation of the owner, are deemed to infringe upon Authors' rights:

- Placing in circulation one or more copies of a computer program, knowing or having the possibility of presuming their illegitimate nature.

- Having one or more copies of a computer program for commercial purposes, knowing or having the possibility of presuming their illegitimate nature.

- Placing in circulation or having for commercial purposes any instrument whose sole use is to facilitate the unauthorised suppression or neutralisation of any technical device used to protect a computer program.

The law provides for actions and procedures that not only may be applicable to cases of infringement of exclusive exploitation / patrimonial rights, but also cover and encompass moral rights; additionally, protection is offered both if the rights in question correspond to the author and if they correspond to a third party that has acquired them (exclusive licensee, assignee).

The owner of the rights may demand that the unlawful activity by the offender cease, request protective measures and claim compensation for the material and moral damages caused.

9.5. Other measures of defence

Apart from the protection under copyright law, the owner of the exploitation rights to a work whose rights are breached by a third party may have other courses of action.

The most relevant among these are:

- **Contractual law**. In the event of a breach of the Authors' rights derived from a breach of a software user licence agreement (e.g. an EULA), it is also possible to resort to the law of contract (obligations), as sue the licensee for breach of contract. The court will thus not only look at the breach of copyright, set out in the law, but also the wording and interpretation of

the contractual dispositions (e.g. express prohibitions on copying, distribution, reverse engineering, or obligations to make payments).

- **Criminal law**. Doctrine has traditionally considered that the Authors' rights, recognised to the author or owner, are also susceptible to criminal law protection. This has been reinforced with the implementation of the EUCD. While provisions vary among jurisdiction, criminal law establishes both fines and prison time for breaches of copyright for lucrative (commercial) purposes.

Examples in Spain and the UK

Article 270 of the Spanish Criminal Code expressly establishes penalties of up to two years in prison for those that "for a profit and to the detriment of a third party, reproduce, plagiarise, distribute or publicly communicate works without the authorisation of the owners of the relevant rights".

In the UK, penalties range from imprisonment for up to two years, to fines and forfeiture of infringing material and equipment for making infringing material. The relevant provision in relation to public communication states: "A person who infringes copyright in a work by communicating the work to the public (a) in the course of a business, or (b) otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, commits an offence if he knows or has reason to believe that, by doing so, he is infringing copyright in that work."

The same penalty is applied to those that "import, export or store copies of such works" and to those "manufacturing, placing in circulation or possessing mediums specifically destined for facilitating the unauthorised suppression or neutralisation of any technical device used to protect computer programs", as we have seen above.

The activity in question seems now solely to require that a profit be sought, i.e., the pursuit of a monetary advantage, which may be simply not having to pay market price for such products. It should also be noted that it is also unnecessary to pay a price to incur the crime. It may be a matter of a mere exchange or free assignment.

This is a subject that should not be underestimated, as the public powers are beginning to act against practices infringing upon Authors' rights due to the pressure exercised by groups of rightsholders.

Example

For instance, in 2008 there were thirty arrests in Spain of purchasers of illegal programs distributed on CD-ROM. The operation has been the result of the investigation of the lists of clients obtained by the police following the dismantling of a network that offered unauthorised copies of software over the internet and that was denounced by the BSA (Business Software Alliance).

10. Conclusion

Throughout this module, we have reviewed the concept of Authors' rights and copyright, and its specific application to software as work with very particular characteristics. We have introduced concepts, analysed authorship models and studied in detail the rights granted by the system to authors. Versus the monopoly of the author or rightsholder, we have commented on the exceptions and limitations inherent in software. We have also commented on the measures against infringements of Authors' rights.

Throughout this journey, we have conducted an analysis in parallel of the implications that the Authors' rights have for the free software development model. Remember that free software, and copyleft in particular, is a means of licensing that becomes a "patch" on the copyright system, devolving to users the freedom that the exclusive rights granted under copyright regimes take away.

However copyright is fundamental for the protection and safeguarding of copyleft: only on the basis of Authors' rights/copyright will a free software developer be able to prevent the misuse of his/her work, in breach of the licence terms (e.g. privatising GPLed software).

> Legal actions taken by the rightsholders of Netfilters or Busybox against infringers are fully grounded in copyright law and the defence of the authors' exclusive right to determine how a work is exploited. See: gpl-violations.org and Second Round of GPL Infringement Lawsuits Filed on Behalf of BusyBox Developers

We hope that, upon completing this module, the objectives set at its onset have been met: mainly, acquiring a comprehensive vision of the current system of protection of works – and software in particular – by Authors' rights and copyright. Although this is not all: it is of special importance to us that not only theoretical knowledge have been acquired, but also the understanding of the philosophy underlying the method of protection of works by the Authors' rights system and the enormous relevance it has for studying the whole free software and content movement.

Finally, we believe that the reader must bear in mind that Authors' rights/ copyright are not isolated from the large changes affecting the modern world. As we have seen throughout the module, but especially in the section on legal protection of technological measures and rights management systems, Authors' rights are being adapted to the technical revolution, and TPMs are becoming an essential element in the protection and management of the rights of the owners to the works.

The future of Authors' rights/copyright as a protection system for software is difficult to predict. As we shall study in further detail in relation to patents, in Europe the large multinationals (who are in practice the main owners of exploitation rights) consider that the copyright protection system is not appropriate and are requesting the application of the software patents system. They believe that the problem lies in the very nature of the Authors' rights/copyright system, which, as we have seen, does not protect the underlying ideas and inventions of a computer program, allowing for the coexistence on the market of computer programs with different source codes but with identical functions.

Trademarks and patents

Index

Introduction

In this module we will present the legal protection of other types of intangible property: trademarks and patents. In continental legal systems, these are generally referred to as "Industrial Property rights".

First, we will look at how trademark law protects the use of distinctive signs on a general basis, how trademarks are used and protected on the internet, in particular in relation to domain names, and in relation to software.

Second, we will look at patents and how they are used to protect "inventions", and the problematic issue of software patents and their relationship with free software.

1. Trademarks

Trademark law within the European Union consists of both national laws, that are harmonised to a certain degree on the basis of the EU Trademark Directive (First Directive 89/104/EEC of the Council, of 21 December 1988, to Approximate the Laws of the Member States Relating to Trade Marks), and there is also a Community Trademark system that covers all the countries of the Union (Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark and Commission Regulation (EC) No 2868/95 of 13 December 1995 implementing Council Regulation (EC) No 40/94 on the Community trade mark).

1.1. Trademark basics

A trademark is any sign susceptible of graphic representation serving to distinguish the products or services of one company from those of the others in the market.

Trademarks

Products: software, such as Linux®, Mozilla® Firefox® or MSWindows®; or hardware, such as Macintosh®, Hewlett Packard®, etc.

Services: computer program development services, the Red Hat® software support service, IBM® consulting and integration services, etc.

The principal function of a trademark is to identify the value of products and the organisations that produce and commercialise them and to distinguish them from others in the market ("distinctiveness" or distinguishing quality of the trademark). A trademark not only protects its owner but also consumers and the proper functioning of the market in general: consumers distinguish products due to the identifying function of a mark, and its association with an organisation. Consequently, the value of the trademark is that acquired in commerce, i.e., that received from the consumers and recognised by the players in the market. Taking advantage of the prestige of another mark and the associated company is therefore prohibited. Ultimately, trademarks seek to avoid the "*risk of confusion*" of products and services in the market, including the "*risk of association*" between companies.

Although the main function of the trademark is to indicate the **business origin** of a computer program, trademark law may offer a basis for the indirect protection of the **product identified**. This would be the case, for instance, in the situations shown below, where the following may be prohibited:

- The modification of a program and its subsequent marketing with the same distinguishing mark.
- The commercialisation of software removing the trademark of the owner that was included with the programs and putting on another (passing off).

A company such as Red Hat can use its trademark to exercise a monopoly over the versions of the free software it distributes. By doing so, it can offer certain guarantees of quality for its versions (for instance, a guarantee that there are no viruses in the Red Hat® Linux Enterprise) and would distinguish its installation and integration tools and support services.

Trademarks may be of **different types**:

- **Denominative** (one or more words).
- **Graphic** or "figurative" (a drawing, letters or figures or combinations thereof).
- **Mixed** (a mixture of words and drawings).
- **Tridimensional** (the form of an object: for instance, the Coca-Cola bottle or the Michelin man).
- **Sounds** (the Nokia sound of a mobile phone).
- Any combination of these.

> **Supplementary content**
>
> Normally, the trademarks associated with a computer program would be denominative, graphic/figurative or mixed, as they are to be visualised on screen.

Trademarks must be **distinctive**. On registering, there are certain absolute and relative grounds for refusing the grant of trademark rights:

- **Absolute grounds**: denominations which are generic or descriptive (i.e. not distinctive), deceptive, consist of official emblems, or are against public policy.
- **Relative grounds**: applications for a mark which is the same or similar to other previously registered (or otherwise valid) marks in respect of the same or similar products. In this case, the registration process enables prior mark holders to object to the registration of the new mark, and this objection can be either negotiated or appealed by the parties.

> **Supplementary content**
>
> Worldwide, laws tend to prohibit the registration of **generic marks** (such as the trademark "Software") and **geographical names** (with the exception of appellations of origin, which have a very specific regime).

Trademark protection is granted in respect of **certain categories of products and services**, as indicated in the application documents for registered trademarks or as claimed, in relation to unregistered trademarks in the UK/US. There is a classification of products that has been agreed at an international level (the *Nice Classification*[1]).

[1]The Nice Convention for the international classification of products and services for trademark purpose seeks to provide information on trademarks at a national and international level, so that the signatory countries use a sole classification for administrative purposes in the trademarks filed at their registries.
The most common classes for software are 9 (for software as a product), 42 (for software services) and 45 (software licensing). Business services on the internet, such as ecommerce, can fall under the classes 35 (a catch-all for business in general) or 38 (telecommunications services), though it is often more relevant to apply for the classes of the products that are actually sold online (books, software, holidays, etc.).

Therefore trademark legislation tends to allow two identical marks to exist simultaneously if they apply to different products or services, in order not to exhaust usable words (the Nice classification referred to above is important for these purposes). In this sense, the "IBM" trademark for programming services is not the same as it would be for dairy foods, if this existed. Precisely, in order

> **Supplementary content**
>
> The European Community trademark registration process allows applying for up to three classes for the same price.

that a distinguishing mark not be limited to a single series of products or services, it is advisable, in the case of doubt, to include a greater number of product classes, although this would imply greater costs in fees and procedures.

Trademark rights are **territorial**. As with patents and as opposed to author's rights, legislation tends to establish that a trademark must be registered at the relevant trademark offices in a given territory to be able to claim exclusive rights, and it is necessary to pay a series of administrative fees for it to be effective over time. Unregistered trademark rights may arise in certain jurisdictions through use, such as the UK and the USA.

1.2. Duration and exclusive rights

The duration of a registered trademark is usually **ten years from registration**, notwithstanding its renovation in subsequent ten-year blocks, which may be done indefinitely provided fees are paid and legal requirements are met. Nonetheless, trademarks must in practice be used (under penalty of "lapsing" in case they are not used for five years).

Trademarks grant owners an exclusive right to use a mark to distinguish their products or services in the market with respect to similar products or services of other companies. These exclusive rights authorise the owners to prohibit third parties from marketing similar products or services under the same mark or under a similar mark that could mislead the public.

The trademark owner may therefore prohibit, among other things, the following, without their prior consent:

- Placing the mark on products or their packaging.
- Offering products, marketing them or storing them for such purposes, or offering or providing services under the mark.
- Importing or exporting products with the mark.
- Using the mark on commercial documents and in advertising.
- Using the mark in communication networks and as a domain name.
- Placing the mark on wrappers, packaging, labels or other means of identification or decoration of the product or service, or manufacturing or providing these wrappers, etc. that may be used to perform any acts prohibited in accordance with the preceding points.
- Removing the mark (although they cannot prevent them from adding their own distinguishing marks or signs separately, as long as doing so does not undermine the distinguishing capacity of the main trademark).

Nonetheless, third parties may use, without the consent of the owner of a mark provided it is done "in good faith" and does not constitute "use as a trademark":

- Their full name and address.
- Indications relating to the type, quality, amount, use, value, geographical source, time of production of the product or service rendered, or other characteristics.
- A third party trademark, if the purpose is to indicate the use with respect to a product or service, especially in the case of accessories or loose parts, provided such use conforms to fair industrial or commercial practices.

As with patents and author's rights, trademarks are also subject to the concept of **exhaustion of rights** for products marketed in the territory where the trademark has been registered. In other words, when a product identified with a trademark is sold, the owner cannot demand its return based on a monopoly of the trademark or prevent it being resold (e.g. in second hand markets).

1.3. Acquisition of trademarks

In some countries, the rights granted by the trademark are acquired through registration, with certain exceptions relating to well-known trademarks (trademarks known in the relevant sector of the public to which the products or services are directed) and renowned trademarks (trademarks known by the public in general).

In other countries, on the other hand (for instance, in English-speaking countries), trademarks can be acquired with use; registration itself is a mere formality with evidentiary and documentary effects.

As trademarks are territorial, various types of trademark may be obtained: national trademark, international application or community trademark.

1.3.1.   National trademarks

Every country has its own trademark office (except the countries of the Benelux, which share a common office) and it is necessary to submit trademark applications separately in each office for the protection of the trademark in that country. This usually requires some simple formal requirements to be met, and the payment of an administrative fee (application fee, concession fee, renewal fee, etc.).

The application procedure varies depending on the trademark office of each country. Basically, they try to filter out applications that do not meet the requirements established by law. The process starts with the filing of documents, followed by the publication of the application in the relevant trademark bulletin. Later, a term for objections commences and, finally, the trademark is either granted or denied.

Supplementary content

It would be fair to use the Linux® trademark to say that a product is "built to run on the GNU/Linux operating system" as this is merely descriptive of the product, and not used to commercialise the GNU/Linux system.

Supplementary content

Marks are often identified by the ® sign when registered and the ™ sign when unregistered.

Trademark rights arise from the date of application for the mark, and a trade-
mark applicant is also entitled, when requesting the same trademark in other
countries signatories of the Paris Convention, to ask for "international priori-
ty", going back to the date of original grant in the first territory. International
priority is given for a period of six months, and is not subject to extension.

1.3.2. International applications

Internationalisation of a mark country by country is expensive and compli-
cated (it implies following a separate procedure for each country). Therefore,
in 1891 the Madrid Convention was executed in relation to the international
registration of trademarks.

An international application is an international administrative cooperation
system directed to simplifying the steps required to register a trademark simul-
taneously in several countries. Such a process is less expensive than separate
and individualised processes in each country.

The process is managed in Switzerland by the World Intellectual Property Or-
ganization (WIPO), a special agency of the United Nations. The procedure
starts from an existing registered trademark or application (national, commu-
nity, etc.) and extends its effects to other countries (allowing requests to pro-
tect the mark in several countries at the same time) through a single docu-
ment: the international application.

The result is a "collection of title deeds" to a trademark that are individual and
independent.

Fees in relation to the international process vary from one country to another.
The fees would be added for each designated country. This amount would
always be less than the corresponding number of separate applications.

The inconvenience with this system is that, during a period of five years from
the date of registration, an international registration depends on the original
trademark registered or applied for in the country of origin. And if the ap-
plication is denied or if the base registration ceases to be effective (either by
cancellation or as a result of decision by the original office or court order, or
due to voluntary cancellation or failure to renew), the international registra-
tion would no longer be protected during such five-year period and may be
cancelled.

After the five-year term, the international registration loses all dependency in
respect of the base registration or base application and each territorial trade-
mark right is a separate right.

1.3.3. Community trademark

The international administrative cooperation procedure was not thought sufficient for the efficient operation of the European Union and the internal market.

Consequently, Regulation (CE) 40/94 by the Council, of 20 December 1993, regarding the community trademark, establishes the possibility of applying for a **community trademark** (often called "CTM"), either directly with the *Office of Harmonization for the Internal Market* (OHIM, in Alicante, Spain), or through the respective trademark offices of the EU member states (to be forwarded subsequently to OHIM).

The result is a single certificate that is valid simultaneously throughout the entire territory of the European Union. Fees are greater than those for a national trademark, but less than the sum of all of them.

> The setback with this system is that, if the trademark is denied in a country based on a prior national trademark, the application fees would be lost and it would be necessary to start again to request another different trademark or request the relevant remaining national trademarks in which there are no equal or similar precedents.

Procedure

The procedure of examination of a CTM application may be schematically summarised in the following seven stages:

1) Presentation of application.
2) Preliminary examination and agreement on presentation date.
3) Examination of other formalities (fees, classification, priority, aging, etc.).
4) Search for precedents.
5) Examination of absolute grounds for denial.
6) Public announcement of application and period for opposition.
7) Issue of certificate and registration with community trademarks registry.

Of course, the risk of denial of grant is higher because the holders of any prior identical or confusingly similar trademark registered or recognised in any of the EU states can object to the CTM application.

1.4. Trademark assignment and licensing

Trademarks may be "sold" (or **assigned**, as we say) to others, like other property, so that the recipient becomes the new holder of the trademark rights. This happens, for example, when a company sells off a business division to another, together with the trademarks associated to the products (and production line) that are sold to the buyer.

> Trademark transmission may be carried out separately from that of a company (this is the case of most EU national trademarks or the community trademark). Nonetheless, in some

countries, the default rule may be the opposite: trademarks may only be transmitted along with the corporate structure, what is known as assignment in gross.

However, in order to enable a third party to use a trademark (e.g. a retailer or reseller of your goods), it is more often the case that rights to use the trademark are **licensed**, subject to controls of product quality and use of the mark. Indeed, it is an obligation of the trademark owner to "police" the use of his/her trademark in the market, to protect it against dilution by third parties (use of the mark by third parties that reduces the identifying function of the mark). So trademark licences tend to establish strict conditions on how the mark is used, with termination of the licence in the event of breach.

> Think of the use of the Linux® trademark in distributions of intermediaries such as Red Hat, Suse, Mandriva, Knoppix, etc. in the use of "OSI Certified" for a licence or the use of the "Apache" trademark on web-servers, etc. This type of use requires a licence.

Licences may be:

- For all or some of the products or services for which the trademark is registered.
- For all or part of the trademark territory.
- Exclusive or nonexclusive.

Both assignments and licenses may be registered before the trademark offices, so as to provide notice to third parties of the rights that have been granted. For the registration of the respective licence with the trademarks office to be effective with regard to third parties, it must be submitted in writing, to access such public registry. Annotations may also be made there in respect of trademarks, successions, estates, etc.

In relation to free software, as it is distributed worldwide without a formal licensing process (for most free software packages), free software projects tend to publish a trademark policy to regulate the use of the associated trademark, without it being necessary to request a particular authorisation.

| **Supplementary content** |
| See FOSS project trademark policies such as Mozilla; os-Commerce and MySQL. |

Other projects include trademark-related agreements in the licence itself (for instance, in the Academic Free License, or the prohibition of using the trademark "Apache" in the Apache 1.1 licence).

1.5. Trademark infringement

In the event of infringing use of someone's trademark, as with other intangible (intellectual or industrial) property, the rightsholder may apply to the courts for an injunction to cease using the mark and account for profits made by the infringer. In addition, to support the case and conserve evidence, goods exhibiting the mark and other evidence of the misuse may be seized, and bank accounts of the infringing party may be frozen.

Before applying to the courts, the trademark holder should and usually does send a letter to the infringer, often called a "cease and desist" letter, requesting the infringer to do just that: cease the current infringing use of the mark and desist from any future infringing use.

We have commented, in section 9.4 of Module 2 on authors' rights/copyright, on the European framework for protecting these rights, which are applicable to all forms of "intellectual property rights", including copyright, patents and trademarks.

We have already seen above the list of exclusive rights of the trademark holder, and unauthorised use of the mark by a third party in relation to these acts would constitute infringement. However, it is not always clear what is considered "infringing use". To analyse any infringement through the use of another mark that is the same or "confusingly similar" to a protected mark, and the likelihood of confusion, different criteria are usually taken into account, including the similarity in the overall impression created by the two marks (the marks' words/letters, the graphic impression or look, phonetic similarities, and underlying meanings) and the similarity/ies of the goods and services in question.

> Other criteria that are considered include:
>
> - The strength of the plaintiff's mark, including its distinctiveness and notoriety.
> - Evidence of actual confusion by consumers.
> - The intent of the alleged infringer in using the potentially infringing mark.
> - The degree of knowledge of the user/consumer and care likely to be exercised by the consumer in choosing a product.

On the other hand, certain jurisdictions such as the UK and the US have established protection for users against inappropriate and unfounded allegations of trademark misuse (e.g. making unwarranted threats, such as sending a cease and desist letter in cases where the use is legitimate).

1.6. Trademarks and internet

Internet and new technologies in general have given rise to a whole new series of questions in relation to trademarks. In this section, we focus briefly on a specific issue in relation to trademarks, which is their use and protection online.

1.6.1. Use of trademarks on websites

Use of a trademark on a website generally constitutes "use in commerce". The owner or licensee of a trademark would usually use the mark on a website for advertising an identified product or services relating to the product.

Use on website that has no economic nature may escape trademark prohibitions, however because it is not always clear when a site has economic implications or not (side banners, self promotion, etc.), this issue should be treated with care.

In certain cases use will be purely descriptive (or "nominative") – basically when the mark is used for identifying a product – and is permitted (e.g., "*I use XXXX products*" or "*XXX products are useful for YYY*"). However there is a fine line between a permitted descriptive use and "use as a trademark" for promoting either one's own products or services or those of the trademark owner.

> A use which is not always clear is stating that a person or company has skills and experience in certain technologies or has carried out certain projects using determined products – depending on how this is done, this could be seen as unfairly using the mark to promote the consultant's services.

Unauthorised use on a website would infringe the rightsholder's rights, entitling him/her to request the website owner to cease (and desist) use of the mark, and, if economic gains had been made, a percentage of the profits made by misuse of the protected mark, as we have mentioned above.

One particular issue here is that of territory: the internet has no boundaries, while trademark protection is territorial. So a person could use a sign that is not protected in his/her territory (or for which he/she has protected rights in that territory) but that site is accessible all round the world. So if another person has rights in the same mark in another territory, he or she may claim that the website use is infringing those rights in that territory. This has given rise to a significant number of conflicts between trademarks on the internet, some of which are resolved amicably, while others have given rise to legal procedures, complicated by the issue of determining applicable law and competent courts for deciding on the issue.

While this is not the place to enter into this topic in detail, we note that a certain amount of case law and practical recommendations[2] have arisen in respect of these cases.

---

[2]In particular, WIPO has offered a "Joint recommendation concerning provisions on the protection of marks, and other industrial property rights in signs, on the internet" which can be found at the WIPO site. It intends to facilitate:

- "Determining whether, under the applicable law, use of a sign on the internet has contributed to the acquisition, maintenance or infringement of a mark or other industrial property right in the sign, or whether such use constitutes an act of unfair competition.

Supplementary content

Typical website trademark usage includes:
- in the domain name (see below),
- in advertisements on the website,
- in hyperlinks,
- in metatags and other (invisible) metadata and
- in adwords and similar advertising programs.

Example

The use of a trademark in a personal blog, provided it was not advertising that or any other product (e.g. it is used to describe or identify a product), would not infringe the rightsholder's rights.

Supplementary content

Chillingeffects.org maintains a public list of "cease and desist letters" brought to its attention. You can see an example at chillingeffects.org.

- Enabling owners of conflicting rights in identical or similar signs to use these signs concurrently on the internet.
- Determining remedies."

Particular points or criteria that courts tend to take into account are whether the sites have a commercial interest and activity, the interactivity of the website (online sales, mere advertising), the use of language, currencies and other localisation factors that could indicate that the website is "aiming" at users within the protected territory.

1.6.2. Use of trademarks in domain names

Domain names are seen as a new form of intangible "industrial" property, inasmuch as they have a specific economic and social value, and can be traded. As a means for identifying the "place" where to find a company or its products online, a domain name acquires quasi "trademark" value for that company.

This is not the place to review the governance and other regulatory issues related to domain names, the role of ICANN and national registries, and their policies as to domain name management. We do, however, want to focus briefly on the relationship between trademarks and domain names.

Insofar as a domain name incorporates a protected trademark, we find a conflict between the owner of the domain name and the trademark holder. Obviously, in most cases these are the same person, as companies buy the domain name corresponding to their company or product mark (*Cocacola.com, sun.com, IBM.com*, etc.). However, this is not always the case: third parties register domain names using others' trademarks[3], either to take commercial advantage or to criticise, or for many other purposes.

[3]This led to "cybsquatting", "typosquatting", and other forms of use of third party marks, some legitimate, some not.

In another scenario, persons with the same trademark in different jurisdictions came head to head when looking for an online identity.

As the domain name system is quasi-privately run by ICANN, it took a while for national and international bodies to come up with a process for sorting out domain name conflicts. Today, this is generally dealt with by "*Dispute Resolution Procedures*" – either at international level under WIPO sponsored rules (the *Uniform Domain Name Dispute Resolution Policy* or "UDRP[4]") for generic domain names (.com; .org, .net; .biz...) or nationally in respect of top level country domains (.de, .fr .es, etc.).

$^{(4)}$"The Uniform Domain Name Dispute Resolution Policy (the UDRP Policy) sets out the legal framework for the resolution of disputes between a domain name registrant and a third party (i.e., a party other than the registrar) over the abusive registration and use of an internet domain name in the generic top level domains".

These DRPs set up a process for an (independent) panel to determine if someone is using a domain in breach of – generally – a trademark holder's rights. They are often based on the WIPO UDRP, which sets three criteria for determining illegitimate registration (and thus order the infringer to transfer the domain name to the complainant):

- the domain name registered by the domain name registrant is <u>identical or confusingly similar to a trademark or service mark</u> in which the complainant (the person or entity bringing the complaint) has rights; and
- the domain name registrant has <u>no rights or legitimate interests</u> in respect of the domain name in question; and
- the domain name has been registered and is being <u>used in bad faith.</u>

This has led to a large number of requests to "recover" domain names registered by third parties, and a significant number of decisions on the merits of each case (), by a panel of one to three arbitrators. These decisions are not without criticism from the legal and business community, often for being too "trademark-holder friendly", despite being, on the most part, practical and commonsensical.

In certain cases, the registration of the domain name has been upheld, even if it uses a third party mark, primarily because the registrant has a bone fide purpose to use the domain name (e.g. for criticism and/or parody) or because he or she has a separate but valid right to use the mark.

The arbitrators' decision is subject to appeal, in the courts of competent jurisdiction (not always easy to determine) so as to provide an appropriate right of legal defence (i.e. before the courts).

2. Patents

Module 2 of this course, on Authors' Rights, indicated that authors' rights or copyright protect the manifestation or "formal expression" of a work, for instance a computer program. They do not protect the concept or "ideas" behind the work – e.g. the algorithms of the software – which are separate from its expression.

A patent, on the other hand, is said to protect the "idea" in and of itself, being a technical solution that is independent from the "manner" in which the idea may be implemented. In other words, a patent –an exclusive right to use an invention– grants a monopoly over an abstract thought or idea, not the concrete "expression" of the "idea".

In fact, this statement is slightly exaggerated, as a patent really protects a (technical) solution to a (technical) problem – i.e. the so-called "idea" in fact must have a degree of applicability and implementation, and not just be purely abstract ("anti-gravity flying machine"). In more general terms, the patent protects technical contributions –inventive ideas– enriching the possibilities of persons in the domain of natural forces, for the satisfaction of their social needs.

This section describes the basic tenets of patent law, before we go on to comment on its applicability to software and the controversy of software patentability.

2.1.   Concept and scope of patents

In general terms, it may be said that patent rights are monopoly rights over the exploitation of implementations of the patented invention, granted to the person (inventor) who has created an "*invention*" from which an "*industrial benefit*" may be obtained. The rights are subject to limitation in terms of territory and time.

The rights granted to the inventor are enforced by a document, a certificate requested by the inventor and granted by the state, known as a "*patent*".

Patents require registration: the monopoly rights solely exist upon application for a patent, and clearly only if this is ultimately granted by the relevant patent office. Ideas that are not registered by their creators before being disclosed to the public are not protected by law.

> This is a significant difference in respect of author's rights or copyright, which grant direct and automatic protection to the corresponding work, recognised throughout the world, simply upon creation, thus without any registration being necessary (although in

some cases it is convenient, as mentioned in the preceding chapter, to register author's rights or the copyright to provide evidence of the date of creation of the work and a presumption of authorship).

In general terms, therefore, a patent sets out the contractual relation existing between the inventor and the state, whereupon the state grants the inventor exclusive exploitation rights with respect to the invention, normally for a period of twenty years, during which the latter may obtain return on the investment made to produce the invention and profits to compensate the risk assumed.

In exchange for these rights, the state publically discloses the invention so as to enrich the technological patrimony of the country and compels the inventor to exploit it under certain conditions, to guarantee that the patented technology should actually be used.

> Anyone interested in the patented technology would probably consider it more convenient to obtain a licence from the inventor in exchange for levies or royalties (i.e., an economic compensation for the owner) rather than risk infringing the patent and pay fines and penalties. This compensation would be not only to pay for the patent itself, but also for the additional know-how not described in the patent documents (necessary to implement the patent) and for the certain technical assistance.

The intention behind the concept of patent is to encourage the disclosure of inventions to society. Patents are not just about rewarding inventors but also for encouraging them not to keep their inventions secret. Without this legal protection, the inventor would tend to keep the invention secret, not disclosing anything about it other than its results (i.e., the products it would place on the market), and thus preventing others from building on this idea to create better products and services.

> As applied to software, this would imply that a software patent would need to disclose publicly the idea and means for implementing a given algorithm, including eventually its source code. However, software source code or algorithms tend not to be published in the description of the patent, precisely to maintain the secrecy of the most valuable part of computer programs: their source code.

The disclosure of the invention, although required to be in sufficient detail to allow an average expert in the matter to understand and implement it (one talks of "teachings" of a patent), does not imply that it should make it easy to abuse or avoid the patent, inasmuch as to enable its correct and proper exploitation (under licence).

In view of the wide scope of the patent rights, to avoid the protection of obvious inventions that do not imply any inventive activity, a series of (minimum) legal requirements have been established. The more trivial an invention protected by a patent is, the more detrimental it would be for the state to grant a monopoly on its exploitation. In such case, the owner of the patent would be granted an unwarranted monopoly. It is therefore necessary for government (the respective patent office) to verify and evaluate the patent application requested by the inventor before its concession.

> The decision to protect an invention with a patent involves a calculation of costs and benefits as obtaining a patent involves substantial costs (upwards of 10,000-15,000 Euros in certain cases) and, once it has been obtained, annual payments must be made to the respective patents office to maintain effective the rights to the respective patent registration.

As with trademarks, patent law is national and protection is territorial. In Europe (but not within the scope of European Union law) there is an international treaty called the European Patent Convention of 1973 ("EPC") which regulates the granting of what is generally known as a "European Patent". The European Patent is regulated and managed by the European Patent Office, in Munich, which evaluates and grants European Patents. Once granted, these are in practice a portfolio of national patents and invalidity procedures must be taken before national courts.

2.2. Requirements for patentability: inventions

A patent protects "inventions". But modern legislations tend not to define the term "invention": they merely establish that inventions meeting all formal and material requirements are patentable. The definition of invention is therefore vague.

> In the United States, an invention must be "new", "non obvious" and "useful". In Europe, on the other hand, an invention must be "new", involve an "inventive step" and have "industrial application". The European Patents Office has in practice developed the concept of "industrial application" as it has understood invention to be a technical solution to a technical problem.

Patent protection thus requires an element of "creativity" (similar to copyrights), in terms of "inventive novelty" defined as a technological advance over prior knowledge. Therefore, what is actually protected – the invention, so to speak – is the technical or technological improvement of a state of knowledge.

2.2.1. Patent requirements

For an invention to be granted patent rights, it must meet the following requirements, which are common to most legislation:

- **Novelty**. An invention is novel when not included in the "state of the art" on the date of application. The state of the art is represented by all that which has been disclosed to the public before the date of presentation of the patent application, on a worldwide basis (i.e. in the country where it is requested or abroad), by written or oral description, by use or by any other means.

> Only "prior art" or disclosed knowledge at the date of the patent application destroys novelty, including, with certain exceptions in some countries, the mere local publication in a tiny college in any country around the world, even a few minutes earlier, or the disclosure in the press by the inventor the previous day. Some countries afford a "grace period" to avoid inventors from being deprived of their inventions when they are made public shortly after applying for a patent, normally to test the attractiveness that the invention may have on the market. But that is always the exception.

- **Inventive step**. An invention implies an "inventive step" when it is not obvious, on the basis of the closest prior art, for an "expert" in the matter. Such expert must have an average education in the sector of the invention and have average knowledge and qualities. He or she doesn't have to be Einstein...

- **Industrial nature**. Finally, and as final substantive patent requirement, an invention is deemed susceptible of "industrial application" when its object may be manufactured or used in any type of industry, including agriculture and, potentially, services.

An important difference lies in that, in the United States, inventions are not legally required to have an industrial application or imply a "technical contribution" or have a "technical effect", as we shall later see. Along these lines, the case law of the United States has admitted that inventions may be patented to the extent that they have **specific, useful and tangible results**.

2.2.2. Exceptions to patentability

In Europe there are a series of exceptions or scenarios of non patentability, limiting what may be patented ("*patentable subject matter*"). The most important exceptions are:

- Scientific discoveries and mathematical methods (to the extent that they are all already existent or could not be considered susceptible of industrial use).
- Literary or artistic works or any other aesthetic creation, such as scientific works, plans, rules and methods of performing intellectual activities, for games or commercial-economic activities, and **computer programs** and means of presenting information (to the extent that they are already protected by intellectual property).
- Inventions whose publication or exploitation is contrary to public policy or good customs.

As regards software, the exception (which does not exist in the United States or Japan, but does in Europe) *stricto sensu* is to the extent that the program is considered on its own ("software as such"), but not as a whole and combined with the hardware. In section 3, we will delve further into this matter and will discuss the requirements for the potential patentability of the software implemented on a computer (i.e., in combination with the hardware).

2.2.3. Classes of patents

The invention must always indicate what a given matter or energy should be, or how it should be acted upon to achieve the desired result. In this sense, we may speak of:

- **Product inventions**. These show how a <u>given matter or energy</u> (a machine, for instance) can be.

- **Procedural inventions or methods**. These show how the <u>activity</u> should be in relation to material reality, i.e. how a person should act in respect thereof.

> To the extent that a procedure is patentable when performed by a technical production procedure (a computer, a computer network or device directed by running a program), we would be dealing with "computer-implemented inventions, claimed as procedural patents".

> Examples are seen in the patents of Acacia Media Technologies, relating to the transmission and receipt of compressed audio and video files over the internet. For further reading, see Information Week.

Supplementary content
To the extent that it is permitted to patent a programmed computer, a programmed computer network or other programmed device, we would be dealing with "computer-implemented inventions, claimed as product patents", i.e., a programmed device.

2.3. Procedure for obtaining a patent

There are a series of formal steps to be taken in order to obtain a patent.

2.3.1. Examination

A patent application is filed with the patent office corresponding to the country or area in which protection is sought. The office then verifies patentability requirements in accordance with the following possibilities (which tend to vary from one country to another):

- **Formal requirements**. The relevant patent office checks if the formal requirements have been met when the applicant provides the documents established by law and meets the formalities determined by such office.

- **Substantive requirements** (or patentability requirements). The patent office verifies compliance with the requirements of "novelty", "inventive activity" and "industrial nature".

With certain differences between patent legislation in the various countries, in practice, the stage of verification of "substantive patentability" tends to be twofold:

- Examination of "novelty". During this stage, ideas lacking invention are detected quickly and cheaply, and the work of the experts of the relevant patent office is trimmed down. Initially, what is known as a *prior art search* is performed. A valuation follows, also known as a technical examination of the application, ending in the decision of whether or not novelty exists. Those preparing a technical examination are much more qualified than those conducting the search for prior art. The novelty of the inventions is valued on a worldwide scale (leading to the standardisation of formalities between patent offices).

- Examination of "inventive step". During this stage, once it has been determined that the idea is not part of the "state of the art", the office verifies whether it has a certain inventive nature, a creative and personal value, and that it is not the logical result of prior knowledge.

Once the requirements have been verified, the content of the patent document is classified in accordance with the International Patents Classification (resulting from the Strasburg Convention of 1971), and the application may be published in the relevant official patents bulletin for the formal knowledge of all people. This grants third parties an opportunity to object to the granting of the patent before final concession. At the European Patents Office (EPO), applications are published upon conducting a technical report, i.e., before they are granted by the European Patents Office, extending their publication for some two years as a result of the pleas and observations of third parties. This extends the procedure quite a bit until their concession.

> In the United States, patents are only published after they have been granted, making the process for their grant faster (less than twelve months, but currently up to 5 years due to over work), inasmuch as, during the grant process, there are no pleas or observations by third parties. In this sense, the EU national and European procedures are among the slowest due to the increased amount of bureaucracy, without this necessarily improving the quality of the technical examination.

In principle, a patent is invalid when it fails to meet the above requirements. However, only a judge may declare the nullity of a patent (after filing the relevant appeal before the courts).

2.3.2. International standardisation of formalities in patents application

The standardisation of formalities has allowed the signature of a series of international administrative cooperation treaties in relation to patents, the purpose of which is varied:

- Based on a single document ("international application"), several patents may be obtained simultaneously in several countries (for instance, using the European patents procedure under the European Patent Convention[5], before the European Patents Office). The result is the obtaining of the various certificates of ownership (national) in the countries where protection is specifically requested for the same object.

[5]EPC members: The Convention member states are the following twenty-seven countries: Germany, Austria, Belgium, Bulgaria, Cyprus, Denmark, Spain, Slovakia, Slovenia, Estonia, Finland, France, Greece, the Netherlands, Hungary, Ireland, Italy, Liechtenstein, Luxembourg, Monaco, Portugal, United Kingdom, Czech Republic, Rumania, Sweden, Switzerland and Turkey.

- To reduce fixed procedural costs, the worldwide search for precedents is solely performed once. This is the purpose of the Patent Cooperation Treaty (PCT[6]), signed in Washington on 19 June 1970. This includes partial regulation of the procedure (the "search" and "examination"), and on-

ly the procedures performed by the larger countries, better equipped with technical human resources, such as the United States, Japan and the European Patents Office are accepted.

$^{(6)}$As with the Munich Convention, the Washington Treaty does not create an "international patent", but an "international application" offering the possibility of obtaining as many national patents as appellations made to the states encompassed by such treaty.

- Finally, we must stress the promotion (not yet effective) in Europe[7] of the "community patent", a single certificate for several states, as occurs in the United States for all federal states. In these cases, we are dealing with a true "international patent", and not just an "international application".

$^{(7)}$The European Union seeks to avoid its current situation in relation to the granting of patents, characterised by simultaneous certificates of national patents which may block imports and exports between territories subject to a different monopoly.

2.3.3. The patent document and "claims"

The fact that the novelty of the inventions is valued at a worldwide level has led to the international homologation of formalities, along with the templates used for the application of the patent, the content of the administrative patent documents and the form of drafting them.

The patent document holds the following elements:

- The **first page** of the patent document tends to be common among all countries and must reflect the relevant information of the inventor and the owner, the title of the invention, the date of "international priority[8]", nationality, administrative data from the patents office itself and a summary of the invention (up to two hundred words).
  The summary has no value with the courts, but it does in the context of the world-scale technical databases containing all inventions registered with the most important patent offices.

$^{(8)}$International priority is the essential means of cooperation between several countries in matters of industrial property and means that a patent application, when filed by more than one applicant, is afforded priority and chosen above others for being the first to meet all administrative formalities (in other words, it does not suffice to be the first to come up with the idea).

Under the "union priority" of the Paris Convention, the term for exercising international priority, where applicable, is twelve months. Nonetheless, according the Patent Cooperation Treaty, "union priority" can be extended for a term of up to twenty months.

- **A technical description** of the invention or report. This report must describe the invention (the problem and the solution) precisely, clearly and comprehensively, justifying the request for a monopoly. Its function is to help interpret the meaning of the claims and must contain sufficient instructions for an expert in the specific field of the invention to be able to reproduce it without requiring any additional inventive activity.

For computer programs, this would imply providing enough information in respect of the program specification, but without necessarily contributing to the source code. Although the description is the central part of the patent document, it does not determine

the content of the legal monopoly, precisely as the descriptions are long and complex. They are, however, used by the courts to determine, under the "theory of equivalents", for instance, whether there may be equivalents between a patented invention and another claimed to be in violation of a patent.

- **Drawings**. Drawings are complementary of the description of the invention. As with the title and summary, they are not binding on the courts, they merely serve an auxiliary informative function (some patent offices require that drawings always be attached for their publication in the respective official patent bulletins).

- **Claims**. The claims are the core of the patent: the claims are devised to condense the legally-binding content of the patent in a few lines, briefly and concisely. These are the statements whereby the inventor determines which new elements make up the invention. In other words, in each claim, the inventor precisely defines what has been invented, containing only such new aspects and elements as make up the invention.

2.4. Owners, duration and content of the patents

2.4.1. Rightsholders

In principle, the legitimate right to request and obtain a patent is invested in the "inventors" and their successors, who may be individuals or legal persons.

> As with author's rights, the various national legislations establish a series of rules for foreigners to be granted legitimate rights, pursuant to the Paris Convention (for instance, when having no residence, or no industrial or commercial establishment in the country). In other cases, reciprocity criteria are also applied.

We would also be speaking of:

- Co-ownership: when the invention is made collectively by several persons. In such case, they would all be responsible for obtaining joint patent rights.

- Individuality: if, on the other hand, the invention is made by various people, but independently, the patent shall usually correspond to the person filing the application on the earliest date (provided it is ultimately granted).

- Work inventions: the patent system is somewhat similar to the copyright system (inventions made within the course of employment belong to the employer) with differences depending on the country:
  - Inventor employees. If the purpose of their work contract is precisely inventing (systematic research and professional dedication), the patent will usually belong to the employer. The author of the invention shall generally not be entitled to supplementary compensation,

unless the invention were to exceed the content of the employment contract or relation, or provide outstanding benefit to the employer.

– Normal employees. If a worker makes an invention in relation in the course of his/her normal professional activity at the company and the invention has been influenced predominantly by knowledge acquired within the company or by using means provided by the company, the employer is often entitled to assume ownership of the invention, or at least to a right to its use. In such cases, workers are usually entitled to fair economic compensation.

An employer may also often claim inventions made by workers within one year of the severance of the labour relation.

Some legislations grant inventors a personal right binding them inseparably as *authors* of their inventions (we could speak of a "moral right" of the inventor).

Supplementary content
The European Patent Convention provides the right of the inventor to be mentioned in such capacity in the patent, in cases in which ownership is transmitted.

2.4.2.   Limitations: time and territory

Duration of the patent. Patents usually have a legal term of twenty years, although in some countries, it is possible to extend them in cases where greater costs and risks are assumed. Normally, patents expire when

- Their twenty-year term lapses.
- They are relinquished by their owners.
- The relevant annuity goes unpaid.
- For lack of use.

Once the protection period has lapsed, the invention is incorporated into the body of technical solutions available to all and may be freely exploited.

Territory. The protection provided by a patent is territorial in nature: protection is only granted in the territory corresponding to the office where the application is filed. The fact that the patent is territorial in nature makes it necessary for inventors to request the concession of patents in all countries in which they wish to protect their invention

2.4.3.   Rights granted under the patent

A patent usually grants the right to prevent third parties from performing, without the consent of the owner, the following acts:

- Manufacturing, offering, marketing, using and importing or possession of the subject of the patent.

- The use of a procedure or the offering of its use when the third party knows or when the circumstances evidence that the use of the procedure is prohibited for lack of consent by the owner.

- The offering, marketing, using or possession for such purposes of the product obtained directly from the patent procedure.

- The delivery or offering to deliver means implementing the patented invention, in relation to an essential element thereof, to persons not authorised to exploit it, when the third party knows or the circumstances make it obvious that such means are suitable to implement the invention and are destined for such purpose (unless the relevant mediums are represented by products that are normally available on the market, provided the third party does not instigate the person to whom such mediums are delivered to commit the acts prohibited under the preceding three items).

Exhaustion of rights

Exhaustion. The owner cannot prevent subsequent acts of exploitation (that it has reserved: marketing, use, etc.) by those acquiring products protected by the patent, licensed by the owner or by a third party with their consent, in a certain territory. This is what is known as the exhaustion of rights, a legal precept that is also applicable to trademarks.

There are three types of exhaustion of rights:

- When the exhaustion of the right refers to a single state, it is known as national exhaustion.

- The future community patent regulated by the Luxembourg Convention provides that once the product has been traded in one of the Member States of the Convention by the owner of the patent or with their consent, the exhaustion of the right extends to the territories party to the referred convention. This is what is known as community exhaustion.

- When the exhaustion refers to the entire world (i.e., all states on all five continents), this is what is known as international exhaustion.

2.5. Transmission and patent licences

As is the case with author's rights, only the prerogatives of the inventor-owner of a monetary nature are susceptible of transmission. Not only patents "already granted" can be transmitted, but also patent applications.

Patents tend to be transmissible by any legal means, specifically by sale, transfer, license (of rights) or contribution to a business. The patent may also be used as collateral in a mortgage.

Transmission

Some legislations impose a series of requirements for the transmission of patents, for instance they must be evidenced in writing and be notified to the Patent Office.

Patents are indivisible, which means that they may not be transmitted (as opposed to licensed) in part. Accordingly, it is impossible to transmit a single claim, or transmit the patent or application for only part of the protected territory.

Licences

Due to the "negative nature" of patent rights with respect to third parties (the right to *prohibit* something), more than acts of "assignment" or "transmission" of rights, it is often said that a patent licence is an agreement by the patent rightsholder not to do something: not to sue for patent infringement. In this manner, the licensee has the benefit of exercising all or some of the rights making up the exclusive patent right safe in the knowledge that the rightsholder will not sue. Accordingly, there are authors that understand that patent licences are not merely an authorisation (as we have seen with author's rights), but a waiver of persecution for infringing the patent.

Patent licences may be:

- For the entire territory or for a partial territory. Often, by default, licences are deemed to extend throughout the entire national territory.
- Exclusive or non exclusive. Except as otherwise agreed, patent licences are usually deemed non exclusive and, when they are exclusive, the licensees are authorised to directly exercise the rights derived from the patent and the licensors cannot grant other licences or even exploit the invention themselves.
- By operation of law. These occur when the owner voluntarily offers the patent via the relevant office so that it may be used by anyone who wishes to do so, as a licensee (this implies the payment of lower annual rates for the patent). Such offer may be withdrawn and is presumed to have been withdrawn when the owner of a patent changes.
- For some or all of the rights making up the right of exclusion (manufacture, commercialisation). Contrary to what we have seen with author's rights, in patents the licensee is presumed to have the right to perform all acts making up the exploitation in all its applications.
- Temporal. Again, as opposed to author's rights, a patent licence is presumed to last the entire term of the patent.
- Compulsory or mandatory. If the owner of a patent refuses to grant a licence voluntarily, in certain exceptional cases a compulsory or mandatory licence may be obtained at the courts or through an administrative organisation (Paris Union Convention). Except with "legitimate excuses" (legal, force majeure, etc.), releasing the owner from such obligation, exploitation of a patent must be sufficient to satisfy market demands.

2.6. Combination patents

What happens if the owner or a third party finds an improvement to the invention? The following can happen:

- The owners of the original patent improve their invention. They may request an annexed deed of ownership, known as a patent of addition. This does not extend the patent in time (twenty years) or space (the territory), but to enlarge its content.

- A third party improves the invention, or a new application of the same object, or develops a new invention in the combination of two products/processes that have already been patented. An independent patent may be requested on the prior original patent or patents. Contrary to "addition", in this case, the patents are always different and independent. Their exploitation takes place through cross licensing, which is granted automatically.

- A third party discovers a new idea in relation to part of the prior patent. A patent would rarely be granted in such cases, but could be when it has enough entity in itself to justify cross licensing.

The impact of "prior" patents is such that large firms find it increasingly necessary to join international patent databases to have access to the following data (by order of priority):

- Verify whether an invention is patented.
- Check for potential patent violations.
- Learn which patents have been requested by the competition (i.e., follow up).
- Obtain market information.
- Stay up to date in respect of technological changes.
- Find a solution to a specific technological problem.

> The foregoing is necessary to plan the research itself and, where applicable, to abandon or redirect a project in the event that a third party were to request a patent similar or identical to the invention subject to research and development. Indeed, large computer companies, the developers of proprietary software, constantly resort to cross licensing in the exploitation of their products. IBM, for instance, is the company with the largest number of patents in the world. Far behind is Microsoft, which has had to join the race late, as in its early days, it had relied solely on author's rights and copyright. Being unable to "cross license" patents from the beginning, Microsoft has had to pay out substantial amounts to the respective patent owners, and currently has changed policy in hopes of obtaining a large number of software patents and aggressively joining in the cross licensing game and, ultimately, engaging its competition.

Aspirin

Aspirin, for instance, was discovered to have cardiovascular effects, in addition to its analgesic effects. Analgesic aspirin and cardiovascular aspirin could not be traded separately on the market as their consumer is one and the same.

Example

An example would be an engine patented for a thermal oscillation of between X and Y degrees Celsius, if someone were to discover that a 75% fuel savings could be obtained at Z degrees Celsius.

2.7. Differences between author's rights and patents

There are several differences:

- **Object of protection**: the most important difference is found between the author's rights system and the patents system for the object of protection. While the patents system protects the ideas or new creation with respect to the state of the art, author's rights refer to the embodiment of literary, artistic or scientific creations (i.e. expressed on any medium).

  In relation to software, in terms of computer programs, patents would therefore protect the functions, results, operation or sequences of a computer program, its algorithms, while author's rights would protect the form in which the program is expressed (the instructions performing a given function), i.e., the source code and object code.

- **Requirements**: The patent requirement of "invention" is therefore set against copyright requirement for "originality".

- **Timing**: Author's rights arise from the very moment of creation of the work, without requiring a declarative act or certificate, as is the case with patents. Although we have seen that registration is a means of protection for author's rights (for instance, notarisation or registration with an intellectual property registry) it is mainly as proof of authorship or a procedure formality for taking legal action.

  The consequence of this is that the protection of author's rights or copyrights is weaker, not only due to the fact that the authorship of the work may be challenged more easily in the case of patents, but also by reason of the rights and actions granted to the owner.

- **Duration**: The duration of author's rights is much longer than that of patents, although in relation to computer programs, in either case it is excessive, due to the short duration that computer programs have in practice.

  This means that when the patent is extinguished (normally after twenty years), any third party may exploit a program based on the same ideas expressed differently (i.e., with a different source code) from the program of the owner of the author's rights, which remain in force.

- **Prohibition**: A patent allows the owner to prevent another computer programmer from writing any other source code implementing the same invention (regardless of how differently it is expressed). Author's rights / copyrights do not prevent another computer programmer from writing new code that is similar or entirely different and leads to the same functionalities.

3. The controversy on software patentability

The application of patents to software –"software patentability"– is a disputed matter. Under its system of case law, since 1981 in the United States it has been possible to patent "*anything made by man under the sun*". This may be changing on the basis of the recent "*in re. Bilski*" case (2009), certainly in relation to business method patents implemented in computer programs.

In Europe, however, software "*as such*" is excluded from patentable subject matter under the European Patent Convention and most European national legislations. There has been some discussion in terms of the possibility of requiring that an invention must exert a *controlled use of the forces of nature* to be considered part of a "field of technology" and, therefore, to be patentable. This does not necessarily imply that anything that includes software may not be patentable in Europe, as we shall see below, and this has led to great controversy.

We shall now briefly look into the origins of patent protection of software, to later delve in detail into the current controversy arising in relation to software patents.

3.1. History of the legal protection of software

Until the seventies, because large manufacturers of computer hardware (in which the programs were marketed inseparably –bundled– with the computer) wanted to avoid the public from knowing the interior workings of the technology, business secrets and confidentiality clauses were applied to computer equipment, especially as regards software.

> During these early times, as the computer program is converted, during its final stage, into machine code (object program), which is merely the electromagnetic signals acting physically upon the hardware (the computer equipment) and have a new result, obtained on a physical medium, it was considered that they could be subject to protection by the legal precept of patents. It was so construed by United States case law on several occasions.

At the end of the sixties and during the early seventies, the various national lawmakers and international treaties began to reject patent protection of software. Additionally, as of 1968, the United States antitrust legislation conducted a progressive separation of hardware and software, leading to the dismissal at an international level of the possibility of software "in itself" being subject to patents for the following reasons, which are still valid today:

• Legal. Software was not seen to meet the characteristics established for being the "object of protection" under the patent. For such purpose, it is deemed necessary for there to be human work implying the *use of the forces*

of nature to reach a material and concrete result. A program, in itself, is represented by an activity that is purely intellectual, with no direct application to the field of industrial technique

It is generally thought that computer programs do not represent a solution achieving a given result through the use of natural forces, but are of an essentially intellectual content. In other words, they devise possible solutions to a logical and mathematical problem, concreted in the algorithm, manifested in lists of operations (instructions), translated into electrical signals acting upon the computer. Additionally, the ideas contained by the programs are not always, or necessarily, "new", which is a fundamental condition for obtaining a patent. Furthermore, very few computer programs would pass the test of "sufficient inventive activity" (according to WIPO estimates, a scarce 1% would).

• Bureaucratic. For an invention to be subject to a patent, it must be obtained after an administrative process that, in many countries, tends to be quite protracted up until its concession. The short practical life of the software implies an important obstacle for its creators and owners, who would solely have their products protected after a considerable period of time as of their applying for the patent.

There is also the fact that the possibility of the programs being protected by patent implied practical difficulties for the respective patent offices and their collapse, inasmuch as one of the aspects accounting for a great part of the work of such offices is the verification of novelty and inventive step. In view of the boom of the computer industry, adding another category of invention for software was not desirable, as patents would be granted even later.

• Economic. The procedure for granting a patent is, quite frankly, expensive. Not only due to the expenses implied by the registration of the patent, its renewal and the payment of an annual fee, but also the cost implied by the fees of the professionals (engineers, lawyers, etc.) participating in the matter. This nonetheless does not imply an obstacle for the larger computer companies.

• Political. In Europe, there was a true distrust in leaving open the means of protection of software through patents to the United States, as they already dominated the production of hardware.

The situation led to an initial decision at the international level to exclude patent protection of software, considering it inadequate or undesirable. But that only lasted a few decades.

In spite of the first references in United States case law favouring the patentability of computer programs in themselves, the courts in the United States unanimously agreed that a method that may be developed by the human brain (mental steps) cannot be subject to patent. As computer programs do not relate to physical matters and may be developed by the human brain, they were deemed not patentable.

Other countries (as was the case of France in its Patents Law of 1968) established in their laws a clear and outright exclusion of the possibility of protecting a computer program through the legal precept of a patent. In parallel, the case law of other countries also reflected the position assumed by the legislation (among the relevant of these are the French case of Mobil Oil in 1973 and the German case of the Disposition Program of 1976).

Furthermore, the Munich Convention on the European Patent, of 5 October 1973, already examined herein, excluded software from patentability under its Article 52.2[9].

[9]Specifically, Article 52.2 reads as follows: "Not to be considered inventions for the purposes of paragraph 1, specifically, are: [...] c) plans, principles and methods for the exercise of intellectual activities, for games or for economic activities, and computer programs".

This led to the European countries adopting similar wording in their national legislations.

Spain specifically established, in Article 4.4 c) of the Patents Law of 1986, the following text: "Specifically not to be considered inventions in the sense of the preceding section [defining what is patentable], are plans, rules and methods for the exercise of intellectual activities, for games or for economic-commercial activities, and computer programs".

The position assumed by the aforementioned legal texts has also been reflected in the cases brought before the courts of the various European countries party to the Munich Convention.

In the eighties, the historical debate on whether it was convenient to protect software with patents resurfaced, due to the worldwide pressure of the large United States software development companies (facing the losses that they had already sustained by then due to the pirating of their programs) and their intention to obtain the greatest protection possible for software through the various legal precepts applicable in each case.

The countries sought protection of the software itself, first through specific protection (which failed), and finally through author's rights or copyrights, as we have already discussed in Module 2.

Although the intellectual property legal framework (copyright) does not provide an ideal solution to prevent the unauthorised use of software, it did offer a prompt legal and international response to the desires of the large computer companies. Copyright law was also adapted to limit the possibilities of using reverse engineering (imitation of ideas without copying the code to obtain the same result, modifying or inverting the sentences or logical instructions), which was considered an unfair practice.

3.2. Patentability of software

But are computer programs really "literary" works? What problems are posed by protecting computer programs with author's rights? Creators and owners of computer programs wish to obtain the greatest possible protection for their rights and protection by author's rights does not cover the "ideas" inherent in the computer program (ultimately, the most creative and valuable part of the programs: the algorithm), because author's rights solely limit protection to "the expression".

Besides, we must not forget that computer programs seek a technical result, i.e., they are the technology required to use the computers and are not created to communicate information or thoughts to human beings (which is the ultimate essence of literary works), but rather are designed to communicate with the machines.

So, in spite of it all, the pressure from the large software developing companies on the patent offices led to their granting many patents on computer programs considered in isolation, when, strictly speaking, these should not have been granted. This is occurring not only in the patent offices of the United States, Australia and Japan, but also, more recently, in Europe, where there are more clear legislative limitations relating to the patentability of software.

> Although patents on computer programs in themselves are not permitted in Europe, see for example:
>
> - A computer-implemented patent where, in truth, the only thing novel is the computer program itself (See the FFII site).
> - A patent of software in itself, granted by the European Patents Office.

In the following sections we shall see the extent to which software patentability is accepted around the world.

3.2.1. Software patentability in Europe

In Europe, computer programs themselves have been excluded by law from the scope of protection by patents. However this exclusion is itself limited.

> **Munich Convention**
>
> Article 52.3 of the Munich Convention itself establishes the following: "The provisions of paragraph 2 shall exclude patentability of the subject-matter or activities referred to in that provision **only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such**".

Therefore, the exclusion of the patentability of the software solely refers to the elements in which the protection of the computer program <u>in itself</u> is claimed: when the computer program is the only element making up the patent application. But it does not exclude industrial procedures implemented with the aid of a computer program.

Thus, the patentability of an entire technical procedure in which a part has been implemented by a computer program seems nonetheless to be accepted. In other words, at present, legislation seems to allow software to be patentable **when it forms part of what is the object of larger technological innovations.** These are referred to as "computer-implemented inventions". Patent protection may not be granted for the computer program itself, but to its combination with other elements of the invention, which has "technical" effects.

This is particularly controversial and difficult to apply.

Drawing the lines

In reality, the European exclusion of the protection of software "as such" through the precept of patents is not so simple. Precisely, the problem lies in where and how to draw the lines of when software is patentable and when it is not. In other words, when is software to be deemed implemented in an invention? When is the exception being abused to achieve the patentability of software that, in truth, does not form part of a patentable invention, but rather is independent from such invention?

- When the item claimed is not the program itself, its presence in the claim is not in itself sufficient grounds to deny patentability, if the claimed item has "technical effects". This means that, for instance, machines and manufacturing or control processes run by a computer program must be considered patentable items.

- A program may be integrated into the computer itself, an electronic appliance or device, so that they become inseparable. Examples of this are seen in the first computers, which already incorporated their operating system, in some modems (those based on digital signal processing devices) or file programmable gate array (FPGA) type hardware. Therefore, in cases where the program is seen as another element of the invention, the patentability of the computer program is, in principle, accepted in Europe.

This is also captured in the case law interpretations reached in the specific cases brought before the judges. In several national cases (for instance, the case of Schlumberger in 1981, France; or the case of Seitenpuffer in 1991, Germany) and before the European Patents Office (Viacom, 1986; IBM, 1997), it was understood, on the one hand, that as most important recent inventions required computer programs, their exclusion from the scope of patentability would imply some ludicrous results in practice. Additionally, it was considered that a claim relating to a technical procedure performed under the control of a program cannot be considered as relating to a computer program "in itself".

In principle, building on the exception established by Article 52.3 of the Munich Convention and based on the TRIPS Agreement, the EPO understood that if the claimed object were to offer a "technical contribution" to the "state of the art", i.e., if it were to have a "technical effect" beyond the interrelation between the program and the computer, its patentability should not be questioned merely for the program being implicit in its implementation.

Under Article 27 of the TRIPS Agreement, adopted by the World Trade Organization in 1994, the following are patentable: "all inventions, whether products or procedures, in all fields of technology, provided they are new, imply an inventive activity and are susceptible of industrial application". And adds that: "[...] for the purposes of this Article, any member may consider that the expressions inventive activity" and "susceptible of industrial application" are respectively synonymous with the expressions "not evident" and "useful".

The foregoing position is confirmed by the Appellate Chamber of the EPO in its successive decisions (which must be taken into consideration in the interpretation of European legislations, but are not necessarily binding). In this sense, due to the pressure from large United States companies, a decision by the Chamber recognised that:

Author citation

"A patent may be granted not only in the case of inventions in which a program manages, through a computer, an industrial process or the operation of part of a machine, but also in cases in which the computer program is the sole medium, or one of the necessary mediums, for obtaining a technical effect within the aforementioned meaning, whereby, for instance, a technical effect of that type is achieved through an internal function of a computer under the influence of such program".

The practice of the European Patents Office has recognised that it is possible to patent software by presenting the application drafted in a certain way. Upon the basis of this it has been said that the European Patents Office has granted over thirty thousand software patents, while the Office itself claims only about 5,000. This situation is not very satisfactory as it produces a great deal of legal insecurity and distorts the market, inasmuch as the practical application of patents regulations is not the same throughout Europe.

US impact

This is mainly attributable to the pressure of the large computer companies of the United States, which have been able to "slip through" many software patents as isolated computer programs and intend to continue to do so, although it be under the guarantees of legal relief. Of the software patents granted by the EPO, 75% belong to United States companies, precisely due to the interest and pressure they have exerted in Europe, compounded by the fact that European companies have not known of the use of patents as a means of protecting their products (or, as applicable, as the European companies that did know, considered patents to be complex, expensive and difficult to apply for small companies).

The Amazon one-click, patented at the United States Patents and Trademarks Office (USPTO), is an example of a software patent converted into an isolated computer program. It is nonetheless necessary to recall that such patent has a "cousin" in Europe, as the patent claims at the European Patents Office differ from those of the USPTO. Having requested its annulment, both in the United States and in Europe, the United States patent was revoked in mid 2007 and the European patent was annulled in November of that same year.

National position

In parallel, the patent offices of some member states of the European Union, such as the UK and Germany (whose legislations also contain the prohibition of patentability of computer programs), have also followed the decisions issued by the Appellate Chamber of the EPO to the extent that the respective

patent offices of such member states of the European Union have granted patents on computer programs that have a "technical effect" or resolve a "technical problem".

Example

The English courts, in particular, have been busy in relation to patents. In the fundamental 2006 Aerotel/Macrossan case, the Court of Appeal established a four step test, which changed the UKPTO process for studying computer related patent applications, which seemed to make it more difficult to obtain a software patent (More information about the test on the Intellectual Property Office site). However, with further judicial review in the 2008 *Astron Clinica decision*, the UKPTO changed again its practice (see the IPO site about the decision) and a question has been sent to the EPO widened board of appeal, to reconcile the national and EPO practice.

3.2.2. Patentability of software in the United States and other countries

The United States Patents Law and case law in principle allow the dual protection of software as both "intellectual" property (by copyright) and as "industrial" property (by patent). This is the case both for patents for software, considered in itself, and for computer-implemented inventions.

The United States Patents Office was the first worldwide to accept applications for software patents. Furthermore, the case law of the United States has understood that procedural patents cannot be excluded for all inventions that, in whole or in part, can be implemented with the aid of a computer program.

This position is backed by the case of "Diamond v. Diehr" of 1981, where it was sought not only to patent the algorithm or mathematical formula, but a novel procedure for vulcanising synthetic rubber for moulding, where the intention was not to reserve the use of the known mathematical equation used in the patent: the mathematical formula "forms part of the process as a whole", which is in truth the object of the patent. Since the case of "Diamond v. Diehr", in the United States it was understood that patents extend to the procedure in which the computer programs are involved, provided the procedure upon which the patent application is based is not made up exclusively by an algorithm.

Additionally, as opposed to what we have seen with the doctrine of the EPO Appellate Chamber, in the United States it is not necessary for the patentable invention to offer a "technical contribution" to the "state of the art": it is sufficient for the invention to belong in the "realm of technology" to be patentable. Therefore, the mere fact that an invention uses a computer or computer program is sufficient for it to belong in the "realm of technology", subject to its producing a "tangible, useful and specific result". This further allows the patentability of not only software, but also business methods, which is clearly excluded in Europe.

This has caused terrible chaos at the patents office, which does not have sufficiently trained personnel to quickly analyse the novelty and the inventive step of the programs included in over fifty thousand applications filed per year. As a result, it is claimed that the triviality of some of the software patents granted in the United States is due to a lack of human resources, qualified personnel and searching systems at the relevant patent offices.

In fact, it was not until 1994 that the USPTO hired examiners with degrees in computer sciences. The office tends to dedicate an average of seventeen hours per patent, hardly

enough to consider in detail the patentability of a program. It is for that reason that the granting of a software patent by error is not surprising in this system.

It is now estimated that a patent application takes between 5 and 7 years to process (March 2010).

This has recently been reviewed in the Bilski case, which has questioned the practice of granting business method patents, i.e. patents over business methods when implemented in software.

On the one hand, in the United States, the procedure of examination of the patent applied for is not too in-depth or quality-oriented (in the United States there are no stages of comments, opposition, etc.), and this allows for the patent application to be swift and inexpensive, allowing access to small and mid-size industry (contrary to Europe, where the patent application procedure is much more costly). Such ease is defended by the argument that they may later be subject to appeal at the courts and subsequently reviewed or annulled, inasmuch as the mere fact that someone were to find the same idea as that of the patent in the earlier state of the art would invalidate the patent.

It is also necessary to bear in mind that, although not impossible, a search for precedents is quite complicated for software, especially considering that a computer program is represented by mere writing (this is how the instructions given by the program to the machine are to be seen), just as music, mathematics, scientific articles etc. are forms of writing and it is unthinkable that a human being could have absolute knowledge of all literary works written around the world.

In this case, we are dealing with a system of weak patents, where there is a great potential for litigation, which we understand is not convenient for companies that cannot afford it. This also creates insecurity on the financial markets with respect of the value of patents and the portfolios of "industrial property" of the companies.

Patentability of software in other countries: Japan and Australia

The test that the Australian patents office adopts to determine the patentability of the inventions in relation to software is as follows: verify whether an invention implies the production of a "*useful economic or commercial result*". This posture seems even more open than that of the EPO, as it is much more difficult to determine what type of inventions should be excluded, considering that most such inventions have some "commercial application".

The same thing that has already happened in the United States, where some thirty-five thousand software patents are registered every year (even for the software itself), is happening in Japan. In Japan there is a doctrine that has been traditionally construed in a way similar to that of the "*technical contribution*" used by the European Patents Office. In Japan it is considered that an invention must consist of a very advanced creation of technical concepts whereby a natural law is applied.

3.2.3. Failed EU Directive on Computer Implemented Inventions

In the late nineties, the European situation seemed unsustainable for two reasons. On the one hand, there was great uncertainty in terms of the patentability of software, in circumstances in which the Munich Convention excluded it from patent protection, but the EPO allowed the patenting of products containing a computer program under certain conditions ("technical nature" of the product, "novelty" and "inventiveness").

On the other hand, existing European national case law, developed mainly in two member states (Germany and the UK) had adopted differing decisions on important matters relating to the requirements for obtaining a patent (i.e., in relation to the definition of "patentable matter"). This was indicative that, in the absence of standardisation measures, i.e., a Europe-wide law, the courts of the other member states could adopt solutions that were entirely different when ruling on such matters.

The licensees and the public in general, potential users of patentable objects, had no certainty that, in case of litigation, the patents granted in such a situation would be confirmed. In 1999, the European Commission identified the need for legislative action in this regard. Between October and December 2000, it called for a broad public consultation, the results of which evidenced the lack of consensus in respect of the rules that were to govern software patents: should they be restrictive, as they had until then, or should they follow the permissive line of the United States legislation? This led, in February 2002, to the *Proposed Guideline for the Patentability of Computer-Implemented Inventions [COM (2002) 92].*

The Commission justified the proposed guideline based on the need to seek concerted action in this area to reinforce the competitive position of the European software industry with respect to the United States and Japan, and to avoid their dominance of the market (especially the internet), inasmuch as, otherwise, European companies would be in a position of disadvantage, mainly as regards United States companies, which had already assumed that computer programs were in fact patentable. In principle, the proposed guideline[10] sought to put a stop to European trends of past years, especially those of the European Patents Office, of admitting software patents, and put an end to the legal uncertainty implying erratic case law resolutions within the European Union.

---

[10]As the chapter on the infamous proposed Directive was closed in July 2005, we will only summarise its precepts:

- Standardisation of the various European legislations in this regard and, consequently, of the resolutions that could be issued by the various court orders.
- Mixed protection (complementary) whereby computer programs could be protected by both author's rights and patents.
- Reduction of the large number of trivial patents that had "slipped through" at the European Patents Office and some national patent offices (menial inventions or making insufficient contributions to the state of the art).

- Limited-scope protection, to the extent that the "invention" must make a technical contribution: a computer program applied to a computer (but not a computer program created independently, to the extent that it was protected by author's rights). Along these lines, this would include the software integrated into intelligent home appliances, mobile phones, engine control devices, machine tools, devices of all sorts and complex computer systems.
- Discard the business models or commercial methods of patent protections used in the United States.

Parliament amendments sought to clarify ambiguities in an attempt to define what "computer- implemented inventions" were and what a "technical invention" was. They also attempted to defend "interoperability" to guarantee the use of standards and protocols and access to the information society, defend the "freedom of publication" and avoid the use of the patents system to prevent the dissemination of knowledge and monopolising means of expression, and maintain all legal patentability requirements.

Finally, after a long trip through the European institutions, the bid was rejected by 95% of Parliament in July 2005, the first time this has happened in the history of Parliament; some argued that it allowed for the patentability of any software and others that the amendments proposed did not provide sufficient protection. The current European situation has returned to its earlier uncertainty.

3.3. Advantages and disadvantages of patent protection of software

In this section we shall see the advantages and inconveniences implied by the patent protection of software from the viewpoint of the large computer companies. In the next block of this unit, we shall see the pros and cons of patent protection of software from the viewpoint of free software.

3.3.1. Advantages

Large computer companies are interested in having their software protected by patents for the following reasons:

- Patents protect the "ideas" behind the computer program. Therefore, a third party could be prevented from creating a similar program (even if it were done with a different source code or algorithms) if the computer program implements the same functionalities. Along these lines, the monopoly offered by the patent is much greater than that offered by author's rights and copyrights.

- The employer becomes the owner of a patent in the most direct form. Normally, in terms of patents, the inventions of the workers belong to the employer and the rights in favour of the worker are considerably restricted. Furthermore, any information acquired by the worker from within the company and leading to the invention shall also be the property of the

company, which may assume ownership of the invention or reserve a right to its use.

- In patents law there are no moral rights *per se*. Notwithstanding the possibility that in some patent legislations, the inventor is granted a personal right ("moral right"), in general, with patents, the possibility of the author of the program exercising the specific prerogatives of moral rights (inherent in the author's rights systems) is avoided.

- There is a greater ease of transmission of the exploitation rights to a patent or to grant a licence. This is the case with respect to exclusiveness and the right to grant sub-licences.

"Aggressive" (as opposed to defensive) patents may play an important role in the value of the intangible assets of a company when it comes time to sell. Keeping important aggressive patents also eliminates market competition, although this must be done taking all due care to avoid sanction under antitrust law. Nonetheless, we shall later see how, in the software world, many of the most important companies in the computer industry amass a large number of software patents for "defensive" purposes. To do so, they match the current practice of cross licensing, in compensation of the patents that they breach. In the end, annulling a patent implies time, information and money that many prefer not to spend, especially if they have a strong hand to play.

> For SMEs it is very difficult to create a patent portfolio to compete with an industry dominated by a few protagonists that hold the rights to thousands of patents each. Contrary to the intention of a system of patents that seeks to protect the small inventor or innovator, the entrance barrier into the software industry is raised significantly. Even the supposedly simple act of litigating, to avoid payment for an unjustified suit for patent licences, may endanger the existence of companies without the resources necessary due to the high cost it implies.

3.3.2. Disadvantages

But it is not all advantages; large computer companies also see inconveniences in the software being protected as a patent:

- **The period of protection is shorter**. Patents offer protection for twenty years, while author's rights and copyrights provide much longer protection. But this disadvantage is not such considering that, in practice, computer programs are short lived, as they are made obsolete in no time, and the terms established by both patents and author's rights prove extremely long.

- **The cost of obtaining a patent**. Patents imply very high costs in the fees of attorneys and engineers, and fees at the relevant patent offices. Nonetheless, this disadvantage may even prove to be an advantage for large companies in respect of small software developers, as the latter may

not have the necessary resources to cover the costs involved in obtaining a patent.

- **Term for obtaining a patent**. As we have seen, a patent solely grants the rights following a lengthy procedure (which may easily take up to five or seven years, according to the country where patent protection is sought to be obtained), although it is also true that a series of protections are given from the time of the application and the effects are retroactive to the date of the patent application. Nonetheless, the effects and protections shall always be dependent on the final grant of the patent. On the other hand, author's rights protect the computer program from the very time of its creation, without need for any registration whatsoever.

- **Specific purposes**. Software subject to a patent is protected – by the patent – within the intrinsic limits of the patent itself and is not protected if it is used e.g. for purposes or in a manner not claimed in the patent. Under author's rights / copyright, the software is protected against copyright exploitation for any purposes.

3.3.3.   Attitudes of the software industry

The foregoing has ultimately led to the following practices:

- Patents are applied mainly for defensive purposes, in other words, to avoid other persons from patenting it, especially to enter the game of cross licence agreements (and exchange their patent exploitation rights with those of other owners).

- Owners refuse to grant licences, as they prefer to exclude their competitors: subject to certain conditions, there is currently no legal obligation to grant a patent.

- Owners sometimes only grant licences on the condition that the licensee:
  – Obtains licences to other patents of the owner.
  – Does not develop products that compete with the patent owner.
  – Pays royalties based on sales, not only for patented products, but also non-patented products.

> This would be a substantial problem for free software as it would be difficult to obtain a patent licence, as free software sales tend to be zero and as free software does not control the number of copies distributed (it should be noted that the developers of free software cannot know how many copies there are worldwide, nor do they obtain sufficient economic benefits to pay for unlimited use licences).

- Large companies compensate each other with their large patents portfolios (what are known as cross-licensing agreements to share their large collections of patents). This means that the few companies that may join the game can corner the software market in a particular area, and with

Supplementary content

This would be a great problem for free software, as it competes in several areas of the market, such as operating systems, databases, office environments, etc.

their substantial patent portfolios or funds they can restrict the entrance
of new companies into the market. Their philosophy is to patent as much
as they can and demand as much as they may from others, to maximise
the profits on their extensive patent portfolios, leading to arbitrary raises
in the prices of licences.

As a result, large oligopolies accumulate patents and grant each other licences
to avoid possible claims for the defensive accumulation of patents.

On the other hand, small companies or individual computer programmers
developing free software are barely capable of paying for a patent application
and, quite likely, would be infringing upon many of the patents of the large
companies. Additionally, large companies with invalid software patents know
that, although a defendant may threaten that to have discovered that the idea
for the invention already existed in prior art before the patent application
(and that accordingly the patent is invalid), this defendant would have no
money to start invalidity proceedings and might in any event end up being
ruled against in a patent infringement procedure.

> It is estimated that seeking to invalidate the patent of Acacia Media Technologies, re-
> garding the transmission and receipt of compressed audio and video over the internet
> (which could lead to a de facto censorship of the networks), would cost over one million
> Euros. United States patents USPTO 5132992 and 6144702, and the very similar Euro-
> pean patent EP 0566662 (includes Spain).

We thus see that the current practice of obtaining an extensive portfolio of
patents is truly justified for obtaining defensive patents and cross-licensing
agreements, but not as a means of compensation for the costs invested in guar-
anteeing the innovation. And the war is not only against the large software de-
velopers (such as the powerhouse Microsoft), but also the large hardware pro-
ducers (as is the case with the giant IBM, the company that controls the largest
number of patents granted worldwide, by far). Ultimately, software patents
are aggressively used in practice to fight competitors with legal weapons, but
not to promote better products.

3.4. Free software and patents

The free software development, distribution and adoption model is quite in-
teresting from a marketing viewpoint: it is a key form of fighting against estab-
lished monopolies (Linux against Windows, Mozilla against MSIE, OpenOf-
fice against MS Office, Tomcat against WebSphere, Java against the Microsoft
development environments) and, for instance, reduce the costs for public in-
stitutions which, otherwise, would be completely dependent on the current
licences system of the private companies.

Nonetheless, if a software patent system was approved in Europe, or if it was consolidated in the rest of the world and was "applied" in the sense of having software patents (on the "software itself"), the free software world could increasingly face problems. For free software, the protection granted by patents is misused and abused, as we shall see below.

Let us consider the following items in further detail:

- **Visibility of source code**. The publication and public availability of free software source code allows any company with a software patent to easily analyse whether or not the source code used in the free software infringes upon its patent. It is much easier to conduct a patentability study and determine based on the source code the ideas behind the program to see if any of the techniques used in the programs infringes upon a patent. To the extent that the free software will most likely contain thousands of elementary processes, many of which may be patented, it is almost certain that it will unknowingly infringe upon a third-party patent.

Supplementary content
The exception relating to de-compiling for interoperability purposes established by author's rights and copyrights is provided to allow determining the "ideas" underlying the computer program, in certain cases subject to limitations imposed by law.

  The public availability of the source code on which free software is based simplifies the search for patent violations and makes it more vulnerable to possible court suits and even criminal complaints. This vulnerability may determine that the companies using free software prefer not to publish it, so that the patentability of the software distorts the principle of publicity and openness on which free software is based.

  To avoid this contradiction, there are those advocating for granting immunity from software patent infringement resulting from the publication of their source code, although exploitation should be conditioned to the limitations of the patent owner and, therefore, subject to the relevant licence.

- **Owners and responsibilities**. The fact that with free software there is not a single company owning all the rights hinders the mechanisms of defence in case of litigation for infringement of other patents, cross-licences or the payment of royalties.
  Additionally, the decentralised construction of free software (through many contributions) complicates the establishment of the responsibilities of each developer in the chain and the evaluation of the legal risks of the various contributions. Below we shall comment on the treatment of patents under free software licences.

- **Protection of "ideas"**. Granting a patent on software could be dangerous for future developments, as what would be patented are often merely "ideas". Some ideas (algorithms, in the case of software) cannot possibly be considered inventions, as they are based on concepts discovered over years in the various fields of knowledge and that are now applied to the computer world. The cost and risk associated with a patent, although mis-

takenly granted on an invention that is not in fact new, could prevent any
development requiring the use of the underlying concept.

An algorithm, especially, as it is a sequence of instructions destined for the performance
of a specific task, may encompass both "technical" and "non technical" processes. But
analysed in abstract and in terms of pure logic, an algorithm does not have physical
points of reference, as it may be applied to many different functions. Along these lines,
an algorithm should not be the subject of a monopoly. Free software could be limited
in the use of ideas and/or algorithms that, in truth, should not have been patented for
going against the principles upon which patents should be based.

- **Incremental innovation**. Computer innovation is not achieved by great
  leaps based on brilliant inventions, but is mainly incremental. Any ap-
  plication contains many small techniques and practices that, if patented,
  would imply an unbearable burden on the development and marketing
  of software due to the cost of checking for patents on every detail. The
  amount of patents necessary to produce a single product could be in the
  thousands.

On the other hand, in other fields of technological development, in which the practice
of patentability is justified, the amount of patents per marketable product tends to be
much lower (for instance, in the case of the pharmaceutical industry, where generally a
single patent is applied to a drug or process).

- **Minefields: impossible searches**. In the case of software patents, detect-
  ing whether a product contains a code subject to a patent tends to have
  a cost that is often greater than that of the creation of the affected code,
  for two reasons:
  - The large number of patents existing in the countries where software
    patents are accepted.
  - The language in which the protected processes are described, which
    differs significantly from the traditional language used by program-
    mers and requires long interactions between lawyers and programmers
    for both parties to understand what is actually protected by the patent
    in question. Even if it were possible to conduct a thorough study of the
    existence of potential problems with the software patents for a prod-
    uct, it would be impossible to guarantee that it would not be necessary
    to license a patent.

On the one hand, it is difficult to conduct extensive and exhaustive searches
due to the amount of potential patents involved and, on the other, it is pos-
sible that after finishing a product, another person or company that has de-
veloped the method earlier, could request a patent. This fact causes an uncer-
tainty that does not exist with other forms of protection of immaterial goods,
such as author's rights.

Unix Compress

An example of this is what occurred with Unix Compress. The program was created in
1984, and in 1985, a patent was granted on algorithm LZW. This made Unix Compress
illegal from one day to the next, until a licence existed allowing its use. The practice of
using a patent precedent search database as a means of information within the process
of development of a computer-related product not only does not exist, but also would
be useless even if it were instated due to its inherent inefficiency. In spite of this, there is

talk of using free software repositories as a precedents base, to identify, if possible, various routines and establish a timestamp (to determine the publication date).

All this affects the development of free software as it hinders the capacity of innovation and development of professionals and companies in this sector. Patenting prior modifications[11] and improvements is tantamount to aborting innovation.

- **Standards and interoperability**. Software patents threaten the increasing importance attributed to software standards (formats, protocols, computer applications interfaces, etc.), to the extent in which they may hinder them.

  The need to find common standards is more urgent every day. To grant a monopoly on a standard would vest its creator with absolute control over the products of all the competition and would prevent the interoperability of computer programs, to the extent that it could infringe upon the patent. Indeed, it would threaten the freedom of dissemination of the knowhow underlying any standard (by monopolising the means of expression). We must also not forget that there is a current search to boost access to the information society and that the possibility of connecting equipment to be interoperable is a means of guaranteeing open networks and avoiding the abuse of dominant positions.

  For instance, the GIF standard could infringe upon patent number 4,464,650, relating to compression algorithm LZW, granted in 1981 by the United States Patent and Trademark Office (USPTO). We should examine, on the one hand, the possibility that a browser might be unable to read files in GIF format, which is commonly used by users. An example of the opposite is the standard for documents ODF (open document format), which is explicitly open to all.

  These limitations would detract from the competitiveness of free software with respect to the "patented" standards of proprietary software and would prevent compatibility with the latter as it would not be possible to use patented formats or interfaces either.

- **Information obligations**. Software patents tend to promote industrial secrecy and encourage the abusive monopoly due to the interest that exists not to publish the source code in the description of the patent. This is inconsistent with the historical purpose of patents of promoting the sharing of knowledge. It also contributes to eliminating innovative competition, which is also inconsistent with its alleged economic effect.

  The publication of the patent should include a description that would allow someone knowledgeable in the area to reproduce the process or invention, to justify the rewarding of the monopoly to the inventor. Nonetheless, as the source code is not included in patent documents, to reproduce a procedure it is necessary to redevelop the source code, which means that the contribution by a patent is, in the best of cases, dubious. For instance, in the case of inventions, it is necessary to provide drawings and diagrams that clearly explain how an element works within the system sought to be patented. In the case of the software, in practice, solely vague descriptions of the matter sought to be patented are added and it is necessary to develop the product to have a concrete and usable program.

In this regard, software patents do not foster research and development in the field of computer programs or the production of programs that better satisfy (in terms of both quality and quantity) the needs of the citizens and companies. The foregoing is completely contrary to the philosophy of free software, for which, due to the complexity of the current computer programs and the greater difficulty of decompiling and re-implementing a program from its object code, it is essential to have access to the source code to be able to improve the quality of the software developed in the world.

- **Interoperability**. It is argued that, in parallel with the exceptions to the author's rights with respect to decompiling for interoperability purposes, patent licences should be free or mandatory and granted without delay to allow for the interoperability between various computer programs. It should also be mandatory that the patent document includes information on the invention that would facilitate the task of the people wishing to adapt a program to another, already-existing one (incorporating the patented characteristics), or the possibility, in the event that patent rights be exercised abusively, of resorting to mandatory licences, and to antitrust legislation to achieve that the owner of the patent does not hold an abusive monopoly.

Supplementary content
Formats. About two years were needed for word processor developers to decompile the formats of the files of Microsoft Office 97 to be able to make their products compatible with the Microsoft products.

- **Costs**. Software patents are very costly and the procedure for obtaining them may be very long and complicated. In fact, it not only requires the payment of substantial fees during the procedure of application and granting, but also the fees of computer engineers and lawyers (and other professionals involved, as is convenient or necessary in the various legislative systems of each country). This is to develop the patent documents (particularly, setting out the claims in precise detail) and procedural follow up, not only by office (administratively), but also at the courts (contentious proceedings), which may imply years of expenses and headaches that are unbearable for smaller applicants. Additionally, the fact that it is necessary to justify that the software patent is implemented in a larger invention requires knowledge beyond mere programming, which implies a complicated assembly of products and a complex technology, i.e., it requires (expensive) qualified professionals.

On the other hand, this proposal makes no sense for free software, as its development generally does not require substantial R&D investments (as opposed to the sizable investments needed in the chemical industry, including pharmaceutical products, the medical industry or highly-specialised machinery sectors), often developed by small companies or independent computer programmers with scarce economic resources and less access to the necessary information to obtain and defend a patent. We must not forget that software in general, although a complex technology, is also open to small developers.

It is also impossible for the patent offices to know who an expert in the matter would be, in order to analyse whether a program is actually the

Recommended website
The Peer to Patent Project: Community Patent Review, http:/ /dotank.nyls.edu/communitypatent/index.php, collaboration between the free community, IBM and the USPTO.

result of an inventive activity or the "normal" evolution of a concept. An idea to improve the expertise of patent offices (in the United States, where software patentability is legal) is to use social networks and peer review systems to identify an "expert in the matter".

- **Timing**. We cannot forget that some of the patent applications pending concession are initially secret and published thereafter (in the United States this usually takes around eighteen months). Nonetheless, during that time, a free software programmer may have developed the same idea in a completely independent manner and be sued for infringing upon a patent that was unknown to them, due to the retroactive effects of the patent (as of the date of application).

4. Conclusions

Trademarks and patents are different and complementary forms of protecting software and giving it (economic) value, however they are very different from author's rights.

- Trademarks protect the economic value of the name and reputation of a program and the project that supports it.

- Patents – supposing they are valid – protect the concepts and functionalities of software against the development and commercialisation of re-implementations of those functionalities.

While patents are anathema to free software, trademarks are specifically used within the community. Not to control the use of the software – usage rights are granted under the free software licences – but to control the quality and protect the reputation of the authors or project that sponsors the software. Established or commercially sponsored projects create "trademark policies" to enable the community to use the mark in a controlled but generally liberal manner. This promotes a wider dissemination of the project with greater legal certainty.

Recommended links

Mozilla: http://www.mozilla.org/foundation/trademarks/policy.html

Ubuntu: www.ubuntu.com/aboutus/trademarkpolicy

These forms of protection and concepts are now recognised by the free software community and incorporated into more recent free and open source software licences, to establish the ground rules:

- Patent grants on contributions, and patent peace clauses against patent claims (MPL, CPL/EPL, GPLv3).
- Trademark "obligations" or prohibitions of use (Apache, CPAL).
- Flexibility as to trademark or patent conditions (GPLv3).

These issues are becoming more and more relevant, as free software moves out of the laboratories, universities and grassroots communities, and moves into the mainstream (enterprise) software industry.

Software licences and free software

Index

Introduction

This module focuses on software licensing, and free software licensing in particular.

Often, the creator of a software program is not its user: given that the law grants certain exclusive rights to the creator of a program in relation to its exploitation, as we have seen in Module 2, the creator must ensure that the user is granted sufficient rights so as to be able to use the software to the extent intended by the parties.

Granting these rights can be done in two manners: assignment and license.

- An assignment is a transfer of rights in an exclusive and definitive manner. This is the closest analogy to "selling" the program as if it were a good.
- A licence is the permission to perform an act (in relation to the work), which without that permission would be an infringement of copyright or a related right. As we will see below, a licence may be exclusive or non-exclusive, and may include several conditions upon use.

Most EU Member States require formalities of some sort (usually a written document) for assignments or licenses to be valid or validly proven.

The copyright legislation of most Member States imposes certain obligations on the contracting parties on the scope of the transfer of rights (e.g. on limitations on the transfer of rights relating to forms of exploitation that are known or foreseeable at the time the copyright contract was concluded or on rules on termination of contracts). Such conditions vary from one Member State to another.

1. Software licenses

In this first section, we look at software licences as a whole, before entering into the core part of the module which is free software licensing. We will also mention software assignments, which in continental jurisdictions are usually written as irrevocable and exclusive licences.

1.1. Concept of software licence

A software licence is a document or legal "instrument" that establishes the terms and conditions whereby the author or owner of the exploitation rights to a computer program (the "licensor", "software rightsholder") authorises the use of the program by another person (the "licensee" or "user").

We often say that a software licence[1] is an agreement, as it consists of an understanding between two parties: the software rightsholder and a user. It is nonetheless hardly ever an agreement that is negotiated between the two of them personally. Normally, it is the licensor that unilaterally establishes beforehand the terms and conditions of the licence, as an "accession" agreement. The user does not or cannot negotiate with the licensor the conditions of the licence, but rather must merely accept or reject them.

> [1]Standard software licences are often called "End User License Agreements" (EULA), such as those that one accepts when downloading and installing a software program from the net, or from a purchased CD. See, for example, Adobe licenses.

In practice, we tend to use the term licence in two senses: to refer both to the software licence agreement (for instance, we speak of "accepting the terms and conditions of the licence"), and to the permission, authorisation or right granted to the user to use the software by the owner of the exclusive author's rights thereto (in this sense, we also speak of "having the licence to use software").

In fact, this dual meaning of the term licence has practical consequences and has given rise to disputes. And the reason for this is that, in certain jurisdictions (United States, United Kingdom in particular), software licences can be either:

- A contract that, in addition to the terms and conditions for the use of the software by the user, may establish other accessory agreements, such as confidentiality obligations, liability, competent courts for resolving any conflicts derived from the licence, etc.

> **Supplementary content**
>
> This has impacts as to contract formation (e.g. the contract requiring acceptance) and interpretation.

- A unilateral statement by the licensor, authorising the use of the software by those meeting and respecting certain conditions and limits, in accordance with the applicable law on author's rights. In this case, the express acceptance by the licensee is not required; therefore, the licence may solely refer exclusively to the right to use the software (and should not reg-

ulate accessory agreements, except as a condition for the exercise of the
rights granted).

The main object of software licences is therefore to set out the conditions that
are set upon the use (exploitation) of a software program, thus the rights that
the licensor grants the user in respect of the software (what they may do with
the software) and the limitations and prohibitions that must be respected by
the user (what they cannot do).

Licences also regulate such other aspects as the following:

- Number of copies and/or licences granted.
- Method of delivery and installation of the software.
- Possible period of installation and acceptance tests by the user.
- Duration of the licence (limited, extendible or undetermined).
- Price of the licence (free, single payment or periodic instalments).
- Warranty period.
- Liabilities and limitations of liability of the licensor.
- Governing law and competent courts in case of litigation.

> In this module, we shall focus our analysis on standard software user licences, whether
> or not customised to the needs of the user. Although it would seem that we have left
> aside "development agreements" (whereby a programmer receives the commission by a
> client to develop software according to their specifications), we should bear in mind that
> these agreements tend to be accompanied by a software licence or assignment in favour
> of the client. That licence, accessory to the "development agreement", is subject to the
> matters explained in this module.

Both non-free ("proprietary") and free software is commonly distributed by
means of the same legal instrument: the user licence. The differences between
proprietary software and free software are evident in the terms of the user
licences that are completely different, especially in terms of the rights that the
rightsholder grants the user:

- Non-free software licences tend to restrict user rights as much as possible,
  reducing them to a limited permission to use the software and to make
  a backup copy. The user is prohibited from copying, modifying or redis-
  tributing the software, and is usually provided a single copy in binary code.

- Free software licences contain a wide array of freedoms for the user, such
  as the freedom to use, copy, modify and redistribute the software. The
  supplier also provides the source code or makes it available to the user.
  Section 4 below sets out a detailed analysis of the content of free licences.

Software and its physical embodiment or medium

Software (either immaterial or a work of the intellect) is distinguished from
the medium in which it is contained (material good): a hard drive, diskettes
or CD-ROM, flash card. An important matter which must be quite clear is that
although users acquire a copy of a computer program subject to a licence,

they are only "buying" ownership of the medium (the CD-ROM or the DVD, for instance) and not the software. In respect of the software, they are only acquiring the right to its use (a user licence), once the terms and conditions of the licence have been accepted.

This means that the user may transfer or sell the medium, and, if it is still during the term of the user licence, this may include the copy of the software (don't forget the concept of exhaustion, whereby the distribution of a copy of the work on a medium terminates the rightsholders' right to control redistribution of that copy). Likewise, the purchase of the medium does not automatically imply having the right to use the program, as the user must first accept the licence.

1.2. Software assignments

As we have noted, an assignment[2] is another means of granting to a third party rights over a software program (or any other work of authorship). However, an assignment is definitive, more akin to a sale, in that the original rightsholder is basically transferring the property of all the rights, irrevocably, to the recipient (known as the "assignee").

[2]Assignments are common in bespoke software development contracts and freelance or consultancy agreements, whereby the supplier assigns all the rights in the created software to the client. "The supplier hereby assigns all rights, title and interest in the [results of the work] to the client, free of liens and encumbrances" is a typical clause.

In continental European jurisdictions the concept of assignment generally does not exist, and the means to achieve the same result is by granting the recipient an *irrevocable, exclusive, royalty free, worldwide license of all the rights in the work, for the maximum duration of rights*. Remember that the creator will always have certain moral rights in a work, and these cannot be assigned or licensed to third parties.

Assignments or exclusive licences may be accompanied by warranties and indemnities that we comment below, just like any other software licence or contract.

1.3. Legal and economic function of licences

Why is the user licence the legal means or "instrument" commonly used by software rightsholders to distribute programs to the users? Basically because they are an efficient way to manage the rights of the software owner, who retains ownership and control over the program while at the same time permits dissemination (whether or not for profit) among users. This is due to the particular nature of software:

- Technical: Software is an immaterial or intangible good of which multiple copies of the same quality may be obtained; it is modifiable, giving rise to derivate works and, indeed, evolves continuously and quickly over time.

- Legal: Software is the object of exclusive author's rights granted by law to its creator, who may authorise its use, copy, modification or distribution, having no legal obligation whatsoever to disclose the source code.

The legal and economic functions of software licences differ, depending on whether they are "traditional" non-free software licences or free software licences.

- Companies developing non-free software benefit precisely from the exclusive exploitation rights granted to them by author's rights legislation. Seeking to obtain the maximum economic return on their software, non-free companies usually base their business model on the commercialisation or "sale" of copies: the more sold the better. Therefore, non-free software licences are traditionally restrictive in terms of content and scope of the rights granted to the user in respect of the software (no copying or modifying, no redistribution, no renting) and are very protective of the exclusive "reserved" rights of the author. It is basically and merely a "use" licence.

- In free software, licences have the same function, but an entirely different purpose. They are used to grant rights and establish obligations, but not to reserve the exclusive rights of the supplier or to commercialise the largest possible number of copies, but to grant and guarantee the rights of the users to use, modify, adapt, improve and redistribute the software. If economic benefits are sought, it is not through restricting user rights, but usually following a different business model (e.g. providing services for the software).

Thus, somewhat paradoxically, software licences, which have traditionally been used to restrict user rights, are also an adequate means of guaranteeing the rights of the users of software via the free licensing model. Free software license restrictions are more "conditions" for the user to exercise the rights granted; conditions that do not seek to reserve the exclusive exploitation rights of the rightsholder, but to preserve his/her reputation and guarantee that all users may benefit from such freedoms, thus preventing possible attempts at appropriating the software. We will see below in Section 4 the mechanism and content of free software licences in more detail.

1.4. Legal nature and regulatory framework

As we have seen in this module, a software user licence is a legal instrument. What kind of instrument is it and to what laws is it subject?

Generally speaking, a software licence establishes an atypical legal relationship, *sui generis*, that does not fall within the traditional set of (commercial) relations understood by courts: a purchase, a lease, a gift or a service rendered.

- The **purchase agreement** consists of a transaction whereby the seller delivers something (and the ownership thereof) to the buyer, in exchange for the payment of a certain amount of money (consideration or price). However, precisely one of the main reasons for granting a software licence is to avoid any outright "sale" of the rights in the software – an assignment. A licensor maintains at all times his/her (intellectual) property rights of the software and control of its copies and distribution.

> **Supplementary content**
>
> In the case of shareware, demos or evaluation copies, the licence could be assimilated to a loan, although they cannot be equated entirely: what is assigned is not a thing but a right.

- A **loan or lease** consists of the temporary transfer by a lessor of the possession and right to use something in favour of a lessee who, in exchange, pays a certain amount of money (normally in the form of rent or regular payments) – or, in the event of a loan, for free – and who, at the end of the agreement, must return the item to the lessor. A software licence cannot be entirely assimilated to a lease or loan: in many cases, a licence is granted for an indefinite term, while leases necessarily establish a determinate term for using the leased property. And even in cases in which the software licence is granted for a determinate term, what the licensor is granting the user-licensee are limited rights to an immaterial good, which are must less than those granted under a lease.
  What's more, when a lease agreement ends, the lessee must return the leased property to the lessor. In the case of software licences, although the user is sometimes required to return the copy to the licensor at the end of the agreement, the user often does not return anything at all, but rather destroys, erases and/or uninstalls the program for good.

- A **gift** is where something is transferred for free to another party. Freeware and free software licences are usually granted gratuitously and in fact could be most closely assimilated to gifts (of a non exclusive right, not of the software). The indefinite right to use the software is permitted, free of charge. Also, gifts may be conditional (when something is gifted to someone, but in exchange the beneficiary must meet a condition) just like free software licence grants rights subject, for instance, to copyleft conditions.

- When software is adapted or tailored to the needs of the user, it may also be assimilated to the results of the performance of work or the provision of a service.

Thus, while establishing an atypical relationship there is no legal norm that would specifically and comprehensively regulate software user licences, as opposed to "classic" agreements that are subject to legal regulation in Civil Codes or statute law, a software licence may bear certain characteristics of each of these relationships. Depending on the circumstances of each case, a court could apply directly or by analogy the law applicable to that relationship to

the software license: e.g. from a sale-purchase or lease agreement, the war-
ranties of title (or "peaceful enjoyment"), good condition and operability of
the thing sold or leased; from a lease, the obligation to return a good or ceas-
ing using it when the term expires.

In addition, there is the debate whether a software licence (a free software
licence in particular) is a contract or mere permission. In the first case, the
courts would apply a large body of legal provisions for assisting in solving
any difficulties in interpretation or application of the licence contract. How-
ever contract law also requires formal steps to be taken to ensure formation
of a valid and binding contract: an offer, acceptance and, in the UK, consid-
eration (basically, payment of price or promise). Certainly in the case of free
software licences, there is the difficulty that often there is no express form of
acceptance, nor indeed easily identifiable consideration from the user to the
licensor.

So a more favourable view would be to see a license as a mere authorisation,
as mentioned in copyright law, whereby the licensor authorises (unilaterally,
in the case of free software licences) the users to carry out determined acts
(copying, modifying, etc.) with or without conditions. Thus the conditions
are not contractual conditions but licence conditions, breach of which would
terminate the authorisation and any further act restricted by copyright would
be a breach of the licensor's copyright rights.

In any event, the application of the norms applicable to contracts and the
aforementioned forms of agreements should not occur in a generalised man-
ner, but for specific scenarios, applying them "by analogy" to resolve disputes
derived from aspects that are either not regulated by the licence itself, that are
governed by ambiguous or incomprehensible conditions, or if a clause of the
licence is considered null for breaching an imperative rule.

> It has specifically been said that the norms on purchase agreements may be applied by
> analogy to standard (mass) software licences that are more similar to a purchase, due to
> their terms and conditions (fixed price, indefinite time), but cannot be considered such.

In the end, a software licence is governed, above all, by the terms set out
in the licence document and agreed between the parties and by the general
norms on obligations. And we must also consider that the copyright law does
indeed often regulate, at least partially and indirectly, the possible content of
a software user licence agreement, with priority over the application or non
application of other norms, e.g. as to exclusivity, term and geographic scope.

Finally, in any case, software licenses shall always be subject to certain laws
and other norms:

• Mandatory law: The norms that apply mandatorily to licensor and licensee
  whatever the licence says. If the licence agreement contains a clause that

is contrary to an applicable mandatory rule, e.g. of consumer protection for providing a warranty, this clause will be null and void.

- Dispositive law: Norms governing the relationship in cases where nothing else has been established in the licence agreement. For instance, if a grant of rights is not expressly established as exclusive, by law it is often understood that the licence does not grant any exclusivity.

1.5. Subjective elements: parties to software licences

Two persons or parties are involved in a software licence (individuals or legal persons), who are granted certain rights and obligations. These parties are, on the one hand, the **supplier-licensor** of the software, and, on the other, the **user-licensee**.

1.5.1. The supplier-licensor

The supplier-licensor is the person who grants the licence to the user to use the software, providing him/her a copy of the licensed software. As we have seen, the supplier-licensor tends to fix the terms and conditions of the licence unilaterally, certainly with mass market licenses, and the user-licensee merely accepts or rejects them (being unable to negotiate the content of any rights and obligations).

The supplier-licensor must have sufficient rights in the software, according to author's rights legislation, to be able to grant the licence. As we have seen in Module 2, those who are authorised to grant licences are:

- The author or group of authors of the software (the original owner of its exploitation rights). These may grant user licences insofar as the exploitation rights to the software have not been assigned to a third party.
- A subsequent owner of the exploitation rights.
- A person who is solely entitled to distribute the software (a distributor).

Several comments need to be made:

- **Legal capacity**: authors may grant user licences for their software provided they are of legal age, i.e., they have the legal capacity to contract. Usually, software developers that are underage need authorisation from their parents or guardians to validly grant a licence.

  > As an exception, national copyright laws sometimes allow underage authors to grant licences themselves if they are independent, e.g. "older than sixteen, living independently with the consent of their parents or guardians or with the authorisation of the person or institution caring from them".

- **Multiple rightsholders**. Please refer to Module 2 on the cases of multiple authorship and ownership of rights: the rightsholders may be "joint", requiring the consent of all the authors, or the rights may be collective,

under the control of a single party who has supervised or compiled the work of others, such as an "editor".

- **Derivate works**. Remember that derivate and composite works – based on or including prior works by third parties – may only be licensed to third parties in accordance with the rights granted by the upstream licence on the prior work. If this licence does not allow relicensing or sublicensing, or redistribution in any form, then the new work may not be licensed at all to third parties.

In this context, for example, permissive free software licences such as the BSD or MIT allow any form of relicensing. On the other hand, the GPL only allows redistribution of derivative or composite works ("collective", in US terminology) under the same terms (the copyleft obligations) and indeed does not allow sub-licensing of the original code, but grants a direct license from the licensor to each new user.

- **Owner of exploitation or economic rights**. When the creator of a software assigns or licenses to another person any exploitation rights on an exclusive basis, we talk of a derivate owner or rightsholder, who becomes the person capable of exploiting the software, including therefore adapting it and redistributing it to third parties under a new licence. These rights may also be acquired by inheritance (heirs) or legal provision (employers).

Agreements as to contributions to free software projects sometimes are drafted as assignments of the rights to the project, and grant a licence back to the author to allow them to continue to develop or exploit the software separately. Freelance or software development contracts also tend to include an assignment or exclusive licence grant, so the client has ownership of the result of the commission and, for example, may grant licences to third parties.

- **Distributors**. Just as many manufacturers market their products through distributors (who resell them, for instance, in a given territory), it is also possible for the author or the owner of the exploitation rights to the software to decide to market the software through a network of distributors, such as OEMs (Dell, HP, etc.), who often incorporate the software "as is" in hardware products, devices or appliances. The distributor is bound by a "distribution agreement" whereby it is authorised in turn to issue end-user sub-licences – often in the form specified by the rightsholder – while the distribution agreement remains effective.

Computer warehouses or stores, where consumer software may be purchased, are not usually "distributors", in principle, as they merely sell the medium (CD-ROM, DVD) containing the copy of the software. The user licence is subscribed later, directly between the "manufacturer" of the software and the user (e.g. with a shrink wrap licence).

Warranty of title or peaceful enjoyment

Should the licence be granted by someone without such rights, the assignment or license of the right to use the software would be illegal and null and void.

In such a case, the licensor would have granted a licence in violation of the exclusive rights of a third party who holds the exploitation rights (e.g. the author of a component included in a software package), who may bring legal action to cancel the licences granted

without their permission, prohibiting the use of the software by the user and holding the licensor liable for damages.

The breach of third party rights by the software supplier in principle does not imply any responsibility for the user-licensee in good faith (i.e., a party taking the licence in the belief that the supplier was truly authorised to grant it). Nonetheless, the user may indeed sustain serious harm, specifically the suspension and loss of the right to use the software, as a result of claims or court actions being brought by the true owner. In these cases, the user will have also paid the wrong person for the use of the software.

> Software copyright law itself provides that those who, without the authorisation of the owner, "place in circulation one or more copies of a computer program, knowing of or in a position to presume their illegitimate nature", are deemed in violation of author's rights (Article 7, EU Computer Programs Directive).

Therefore, having sufficient rights to grant a software licence is an intrinsic and *sine qua non* condition for doing so; and anyone granting a licence without having sufficient rights to do so will be liable to the user for any damages they may sustain if they are determined to have acted without sufficient authority to grant a licence. Therefore, it is said that in granting a user licence the supplier must necessarily grant the user a "*warranty of ownership*" or "*peaceful enjoyment*", whereby users are assured that they may use the software legally and that they may continue to use it for the duration of the licence.

> In certain jurisdictions, more than a warranty, ownership of rights in the software is an inherent condition that the supplier must have over the software so that the licence is valid and does not infringe upon third-party author's rights. We nonetheless speak of "warranty of title or ownership" by influence of the law of English-speaking countries, as many software licences are a translation or adaptation of United States licences. Warranty of title: the supplier guarantees that they have the due authority to grant the licence and that no third-party rights are being infringed upon.

Additionally, should the user be a consumer, Consumer Protection Law applies, as we note below, whereby the supplier of software will be liable to the consumer user for the origin, identity and suitability of the software (often, in practice, for both consumers and independent professionals). Under these laws, clauses seeking to limit or exclude such warranty of ownership are generally null and void.

> Many software licences follow the model of English-speaking countries of not granting any warranties on the software, not even a warranty of title, stating that the software is delivered to the user "as is". Many even expressly state that they provide no warranties of title and non-infringement.

> As mentioned earlier, this exclusion of the warranty of ownership is probably invalid in most EU jurisdictions, as the software supplier is required by law to guarantee ownership of the software. It should be noted that the EUPL 1.1 (European Union Public Licence), drafted for the European legal framework, includes a "warranty of title", as does the OSL 3.0 (Open Source License). These licences are discussed below.

1.5.2. User-licensee

The user-licensee is the person acquiring the right to use the software under the licence, according to the terms and conditions established therein (almost always imposed by the software supplier). The main obligations of the user-licensee is to pay the price of the licence (when a paid licence is involved) and respect the user limitations imposed by the licence.

> In the case where the user is a licensee of non-free software, in principle, they usually have few user rights (basically, to run the program, use the application and make one backup copy, if not already provided), while the limitations are many. On the other hand, if the user is a licensee of free software, the freedoms of the user-licensee are much greater and, accordingly, the limitations are lesser: they could use the software freely, and modify and redistribute it, with or without modifications.

Should users be authorised to modify the software and they do, they may become the author of derived work (i.e., of the translation or adaptation of the software), as we have seen in Module 2. Additionally, if a user is authorised to redistribute the software and does so, they too may become software suppliers. This is often the case in free software development.

It is relevant to determine, in a software licence, whether the user-licensee is a consumer or a business, inasmuch as the legal system governing the licence and the legal norms applied to the relationship may vary accordingly, especially, in terms of the validity, application and interpretation of its clauses (for instance, regarding the termination of the agreement or the responsibilities of the supplier).

> Sometimes, the text of the user licence itself contains different rights and obligations depending on whether the user is a consumer using the software for personal use or a business using the software for its business activity. Much "freeware" or "shareware" is granted freely for personal use and subject to payments for business.

Consumers

If the user is a consumer, they are deemed to be in a particular weak negotiating position, which means that they have legal protection with respect to possible abuses by the software supplier. In this case, the licence is subject to the rules of the Consumer Protection, harmonised to a certain degree throughout the European Union, which prohibits abusive clauses. These are provisions that are not individually negotiated and that, contrary to the requirements of good faith, cause a significant imbalance to the detriment of the consumer of the rights and obligations of the parties.

Abusive clauses

Examples of clauses that are prohibited from being included, for being considered abusive:

- Clauses conditioning the performance of the licence to the unilateral will of the supplier: e.g. the right of the supplier unilaterally to construe or modify the terms of the licence, after its acceptance by the user, or freely to resolve the agreement, without notice or indemnification.
- Clauses stripping consumers of their basic rights: e.g. limiting or excluding the warranties that must legally be provided for the software and limiting or excluding their liability for damages caused by defective software.
- Other abusive clauses such as requiring the consumer to accept unknown clauses or conditions, forcing the user consumer to purchase unsolicited accessory goods or services or imposing that, in case of litigation with respect to the licence, courts other than those of the domicile of the user consumer should have the competent jurisdiction or that the licence should be subject to a foreign law, unrelated to the parties.

Additionally, when the user consumer acquires the software user licence over the internet (online), the software supplier must also meet the information obligations imposed by national implementations of the Ecommerce Directive[3]:

[3]The obligations under the national ecommerce law are imposed upon the licensors established in the relevant country. If the licensor is established outside of the European Union, the national (EU) ecommerce law shall solely apply to the licences granted to national consumer users and provided their web site is specifically directed to or has a specific section for that country.

- Before purchasing the licence, certain data must be provided in relation to the licence and the contracting process, in addition to the text of the general conditions.
- After acquiring a licence, the supplier must confirm with the user that their acceptance has been received and documentary evidence provided.

Business or professional users

Although the rules protecting consumers generally do not apply when the user is a business or professional, this does not mean that the software supplier may impose upon such clauses that are unfair or abusive. What in fact happens is that the business user does not have mandatory legal protection, whereby certain clauses are automatically deemed null and void.

However, a clause may be considered null and void, even in respect of business users, if it is considered to be contrary to the general rule of good faith that must govern the performance of the agreements, or a "reasonableness test" in the UK. This will depend on the examination of the circumstances of each particular case and in the end it is the courts who will decide whether the clause is contrary to good faith or unreasonable.

> Certain circumstances shall be considered as relevant when determining whether a clause should be annulled –for being abusive– when the licensee is a business or professional. For instance, whether the licensee is a large or small company, whether there has been a true process of negotiation between the parties, whether the user-licensee has accepted a clause that is unfavourable for its interests, in exchange for another favourable provision (for instance, a reduction in the price of the licence or a right to modify the software, in exchange for greater limitations to the liability of the supplier) or whether the supplier has simply imposed them.

1.5.3. Parties to a free software licence

In the case of free software licences, the traditional positions of supplier-licensor and user-licensee are maintained, however some specific points should be noted.

- First and foremost, the granting of a free software licence implies that its owner shares the exploitation rights with the users. This does not mean that the free software becomes part of the public domain, or that the rightsholders waive their rights. Free software is not software with "no owner". The author continues to maintain his or her status as author of the software and, in particular, maintains his or her moral rights in the work.

- By granting users the rights of to modify and redistribute the work, the user-licensee under a free software licence may, in turn, also become the supplier-licensor of other users, either by relicensing the same software (if they have the right to sub-license), or by licensing software derived from the original.

- Despite what free software licences often say – they tend to state that the software is offered "without warranties" – free software licensors must guarantee that the software does not infringe upon the right of any other software (whether free or non-free). The warranty of ownership and peaceful enjoyment is inherent in the condition of software supplier and is inescapable.

1.6. Objective elements in software licences

By objective elements, we mean those elements of the user licence relating to its object: the content and scope of the user rights. What rights are granted by the rightsholder to the user with respect to the software and subject to

what limitations? As we have already had occasion to note, the rights and obligations of the parties with respect to software vary substantially according to the licence.

In this section, we look at the term and price of a licence, and then the different rights that are granted.

1.6.1. Term

Software licences should establish the duration of the licence grant, i.e., its term. In principle, unless either of the parties were to breach their obligations under the user licence, it should remain effective during the established term. Generally speaking, licences are granted for a fixed term, an indefinite term, or sometimes do not provide anything in respect of term.

- Fixed-term licences. In fixed term licences[4], a specific period is established for the use of the software; n months, n years, etc. At the end of the term, if the licence does not say otherwise, it expires and the user must discontinue use of the software.

  This does not prevent the parties from agreeing later to subscribe a new user licence for the same software. It is even quite possible that the licence itself establishes that, when the effective term lapses, the licence should be deemed tacitly or automatically extended for a new term and so on until one of the parties gives advanced notice of their intention not to extend it any further.

  In the case of demonstration or evaluation software (known as demos), the licence is also usually established for a fixed term. In this case, fixing the term is essential to accomplish the purpose sought with the distribution of this software: for the user to get to know, over a short period of time, its functionalities and, at the end of the period, they may decide whether or not to purchase a complete version of the program.

[4]Licences granted for a fixed term are commonly used for more specialised and complex software applications, aimed at companies that are normally bound by an accessory agreement, such as a consulting or maintenance agreement. In such case, the user tends to pay regular instalments to the supplier as a licence fee.

- Indefinite-term licences. In this case, the software licence agreement expressly establishes that the licence is granted for an indeterminate period, not being subject to any specific term. Users may use the software as long as they meet the terms and conditions of the licence.

  Notwithstanding, some indefinite-term software licences[5] establish clauses that allow one or both parties to end the licence whenever they desire, by giving advanced notice of termination. This can be considered abusive in certain circumstances (see above, in respect of consumers).

[5]Indefinite or indeterminate-term licences are more commonly used for mass market software, especially for consumers, where the user pays the price of the licence on one single occasion.

- Lack of express term of the licence. When a software licence agreement does not specify anything with respect to its term, the licence is not nec-

essarily granted for an indefinite term. In certain jurisdictions, like Spain, in these circumstances the licence is limited to a specific term (five years, in Spain). This is often contrary to the intention of the licensor – who should improve the drafting of the licence!

This is what happened with the GPLv2. Although there may have been arguments to extend the period of the licence, on the basis that limiting their effective term to five years could go against the obvious intentions of the parties and the purpose of the licence, GPLv3, along with other more recent licences such as the OSL 3.0 or EUPL 1.1, now establishes the "maximum duration of rights" as the term.

- Term in free software licences. First, it should noted that free software licences are and should be granted for indefinite terms – which sets the term to the maximum duration of copyright protection. Thereafter, a licence is no longer needed as the software is in the public domain.
  To establish a limited term of duration in a free software licence would imply adding a restriction to user rights (in this case, a temporal restriction), which would be contrary to the very essence of the free software licence: not to limit the use of the software by the user, but to guarantee the freedoms over its use. It is thus commonly accepted that free software licences remain effective in time as long as the user respects their conditions.

GPLv3 the OSL 3.0 and other modern licences, have filled the existing void under the prior version, indicating, for instance, in Clause 2 of GPLv3, that the rights granted under such licence shall be deemed "granted for the term of copyright on the program" and that they are "irrevocable provided the stated conditions are met". Likewise, other licences, such as the Apache 2.0, expressly indicate that they are granted with a "perpetual" and "irrevocable" nature (clauses 2 and 3).

1.6.2. Price

Another essential element of a software licence (at least in a most non-free licences) is the price, the amount of money that the user is to pay for taking the licence grant.

In terms of payment modalities, the price may be paid on one single occasion (lump sum), e.g. upon acquiring the licence. This is typical of mass-marketed software licences. Otherwise, payments can be made in regular instalments: the user makes a regular (monthly, yearly, etc.) payment of an instalment[6] to the supplier. This is typical of software licences for more specialised and complex applications, directed to companies, licences established for a fixed term and regularly bound by an accessory consulting or maintenance agreement, for which the user also pays a fee.

(6)Payment in instalments is now common for "software as a service", whereby the user contracts a (pseudo) licence agreement to use software – often over the web – for a monthly or period payment. We say "pseudo" licence because in many cases the user never in fact exercises any of the copyright protected rights (reproduction, transformation, distribution) but "uses" the services of the software. Basically, the user is paying an access fee.

When the licence may be extended in time, a clause is often included for the review or updating of the rate payable by the user. It is not valid to agree that the review of the instalment should be left to the free will of the supplier, but must be obtained either by mutual agreement between the parties, or referencing an objective index or parameter, such as the "consumer price index".

Licences may be granted for free, without the user having to pay anything for the use of the software. We must bear in mind that we must not automatically identify "proprietary" non-free software with paid software, and "free software[7]" with cost-free software. In the English-speaking countries, this confusion has arisen due to the fact that "free", in addition to "without restraint", also means "cost free".

(7)Free software is nearly always free (gratis), but many non-free programs are also distributed free of cost: Microsoft® Internet Explorer, internet messenger clients such as Microsoft® Messenger, Skype, etc., software demos, shareware or drivers.

Price in free software

As regards free software, we know that the term free does not mean that the program is licensed by the software supplier free of cost, but that it is licensed to allow users to use, modify and distribute it freely.

In the case of the GNU-GPL, the supplier may choose to distribute the software free of charge or in exchange for a consideration (paragraph 5 of the Preamble, and Clause 4 of Version 3); economic compensation may also be required for providing certain warranties on the software, unless required by law to provide those same warranties. Other free software licences, such as the Apache 2.0, expressly state that the licence is granted free of charge: its clauses 2 and 3 state that the licence is granted royalty-free.

Nonetheless, although the free software supplier may be entitled to require economic compensation, it is most common that the software is distributed free of charge and that the price requested is minimal (the term "residual" price is used), solely to cover certain expenses, such as the making of the copy, its delivery on a physical medium, etc.

Should an economic benefit be sought with the free software (which is not always the case), the supplier would not obtain it as much by charging a price for the distribution of copies, but rather for rendering services for the software, such as updates, consultancy and the marketing of copies of software based on free software. And on the market there are solutions based on free software that, considering the user licence on the software and the relevant consulting and/or maintenance services, have a high price (see, "Red Hat" as an emblematic case, and many others).

The fact that the supplier of free software cannot base their economic benefit on the price of the copy seems obvious: if the users are allowed to distribute the software freely, the supplier loses exclusive control over the copy. It does not make sense to charge a high price for the copy when the users could in turn distribute – online or on CDs – as many copies as they wish.

1.6.3.   Rights, prohibitions and limitations

In prior modules, we have seen that author's rights or copyright legislation grants a series of important exclusive rights to the author of the software or the derived owner of the exploitation rights: the right to reproduce, transform and distribute (including, for our purposes, publicly communicate) the software. They decide what to authorise, when and how.

Additionally, we know that the software licence is the legal instrument whereby the software rightsholder allows its use by third parties, the users. The user licence therefore has an essential content:

- On the one hand, it establishes the rights that the rightsholder grants the user to the software: what the user may do with the software.
- On the other, it also establishes certain prohibitions and limitations on user rights, which the user must respect: what the user may not do with the software, and the conditions applied to its use.

We refer to Module 2 on authors' rights as to the scope of the rights that are exclusive to rightsholders and thus potentially subject to licence conditions:

- Reproduction.
- Transformation.
- Distribution (including rental).
- Public communication.

Adobe® Photoshop®

If you obtained the software and any required serial number(s) from Adobe or one of its authorised licensees and as long as you comply with the terms of this agreement, Adobe grants you a non-exclusive licence to install and use the software in a manner consistent with its design and documentation and as further set forth below... General Use. You may install and use one copy of the software on up to the permitted number of your compatible computers as long as, when required by the software, you present a valid serial number for each copy.

Generally speaking, all rights that are not granted in a licence are reserved, i.e. not granted. To reinforce this, licenses often add specific prohibitions:

Adobe® Photoshop®

4.3 No Modifications. Except as permitted in Sections 2.7 or 16, you may not modify, adapt or translate the software.

4.4 No Reverse Engineering. You will not reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the software except to the extent you may be expressly permitted under applicable law to decompile only in order to achieve interoperability with the software.

4.5 No Unbundling. You may not unbundle the component parts of the software for use on different computers. You may not unbundle or repackage the software for distribution, transfer or resale.

4.6 No Transfer. YOU WILL NOT RENT, LEASE, SELL, SUBLICENSE, ASSIGN OR TRANSFER YOUR RIGHTS IN THE SOFTWARE, OR AUTHORISE ANY PORTION OF THE SOFTWARE TO BE COPIED ONTO ANOTHER INDIVIDUAL OR LEGAL ENTITY'S COMPUTER EXCEPT AS MAY BE EXPRESSLY PERMITTED HEREIN.

It is common for rightsholders to attach conditions on the exploitation of the software. Some of these are reasonable (payment of a price, maintaining copyright notices), others may seem unreasonable or just strange: e.g. licences that forbid the publication of the results of any benchmark or analysis of the software. While these conditions are often outside the realm of copyright protection scope, if the licence is deemed a valid and binding contract, these provisions will be seen as contractual obligations binding on the licensee.

> The most well known and highly debated condition in the free software domain is Clause 2.b. of the GNU-GPL that contains part of the copyleft obligations:
>
> "b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this licence."

Applicable legislation itself may provide that, in the absence of express terms to the contrary, software user licences are granted to the user on certain terms.

> In Spain, for example, licences are, by default:
>
> • Non exclusive. In other words, they do not grant the right to use the software to a single user, but to a number of them.
> • Non-transferable. The user cannot convey the licence to third parties, which also implies a prohibition to sell, rent, grant sub-licences or give away their copy, except with express authorisation from the supplier.
> • Solely to satisfy the needs of the user. Without express authorisation, the user may solely use the software strictly for their own personal use, not to provide services to third parties.

1.7. Warranties and liabilities

A very important detail in supplier-licensor and user-licensee relations is the determination of the legal consequences derived from an incident with the operation of the software, especially considering the relative instability of software (it is susceptible of malfunctioning, mis-configuration, etc.) and the material inconveniences and damages that a user may sustain as a result of software issues (especially, the companies and entities whose activity depends on the proper operation of their information systems).

Intellectual property laws do not cover this aspect, but merely regulate the exclusive rights to the software. Nonetheless, various norms apply in all countries: Contract Law, rules on warranties in other agreements (such as purchase, lease or service agreements, applicable by analogy to the software licence), norms protecting consumers, etc., could oblige suppliers to assume certain warranties and liabilities with respect to the user, without the possibility of their being eluded by the licence.

1.7.1. General considerations

Software licences tend to regulate the rights of the user – and the consequent obligations of the supplier – in case any incidents were to occur with the software: malfunctioning, miscellaneous defects or if it does not match the characteristics that the supplier boasts in respect thereof and which led the user to purchase the licence.

When any of these circumstances occurs, the user is prevented from using the software or from using it for the purposes that led to acquiring the licence. Should the user not be at fault for the incident, a principle of justice tells us that the supplier-licensor should assist the user and put an end to the incident: we would thus be referring to the supplier having to provide the user a **warranty** in terms of conformity and the continued operability of the software.

> **Warranties**
>
> Warranties are the commitments or obligations assumed by the supplier-licensor in favour of the user, with respect to the conditions (characteristics, services, correct operation) that must be met by the software subject to the licence. This means that if the software does not meet or at some point ceases to meet such conditions, the supplier-licensor must take the appropriate actions for the software to meet them. Specifically, it should be noted that warranties of conformity and proper operation, whereby the supplier is to guarantee to the user-licensee that the software conforms to its description and will work appropriately during the effective term of the licence.

But what is more, such an incident could have caused damages to the user. We should think especially of the software on which, in practice, the proper day to day activity of a company or professional user depends: one defect or malfunction could paralyse their activity, which would obviously imply damages. If the supplier is "at fault" and, therefore, responsible for the damages suffered by the user as a result of the incident with the software operation, this would require them to provide **indemnity**.

Supplementary content

It could be said that "liability" (an obligation to compensate) is one of the possible consequences of the breach of a warranty.

We have seen that software suppliers tend unilaterally to impose clauses of the licences on the users. Licensors are particularly interested in establishing limitations or disclaimers of warranties and liability with respect to the software.

Nonetheless, in certain cases a disclaimer or limitation clause is not legal. The same principle of justice to which we referred earlier tells us that it would be unfair and/or abusive for the licence to allow the supplier to disregard any incidents occurring with the software. It would be particularly unfair if the user has had no opportunity to negotiate the content of such clauses, but rather were imposed by the supplier-licensor; or when the user has paid a price for the licence.

This situation would be different with licences in which the user-licensee has had the opportunity to negotiate the content of the licence and a disclaimer of warranties and/or liability in favour of the supplier-licensor, in exchange for a balancing item in favour of the user (for instance, a reduction in price or a better warranty in exchange for less liability). This would be the case with specialised software usage licences, highly-priced and adapted to the needs of the user. In such case, the limitation or exoneration could indeed be considered fair, as it would be freely negotiated between two parties in equal or similar negotiating positions.

1.7.2. Warranties

User licences usually regulate which warranties are to be provided by the supplier, their term and how they will be fulfilled: i.e., how the supplier-licensor would assist the user in remedying the incident, by repairing the fault or defect, substituting the copy with another, or refunding the price to the consumer, cancelling the licence.

In any case, the clauses of licences providing warranties, including their possible limitations or exonerations, must respect a series of imperative norms that, in each country, establish the requirement to provide certain minimum warranties with respect to the software.

The minimum legal obligations (warranties) on software are generally:

• The warranty to remedy any hidden defects.

• Conformity with specifications or description.

• Correct operation.

  In the law of English-speaking countries, these are often called:

  • Satisfactory or merchantable warranty. The software must be legally marketable –not be something prohibited– and must be of satisfactory quality, considering various criteria (price, market, state of the art, etc.).

- Fit for a particular (stated) purpose. The software must be fit to accomplish a particular purpose, when the licensee acquired the licence based on the possibility of accomplishing such purpose and the supplier knew or could have known that the licensee wanted to acquire the licence precisely for such purpose.
- Along with these warranties, there is also mention of a warranty of title and non-infringement. This corresponds with the warranty of "ownership", to which we have referred above.

In continental European law: There are different legal classes and categories of warranties as regards those inherent in the law of English-speaking countries. Nonetheless, many software licences, even written in a national language and to apply in that country, refer to the typical warranties of the law of English-speaking countries. This makes the wording of such clauses tend to seem confusing. In any case, the content and scope of the warranties is similar in either case, as are the actions and remedies established in favour of the user to implement them: repair, substitution of the copy or return of the price, cancelling the licence.

1.7.3. Liability or indemnities

Liability consists of the duty of the supplier to indemnify the user for the damages sustained thereby as a result of an error, defect or malfunction of the software, or of its lack of suitability for the characteristics that could be expected thereof.

It may be the case that, by reason of an incident with the software, the user could sustain damages. In such case, it would not suffice for the user that the warranty should be honoured (that the supplier should repair the malfunction, provide a new copy or return the price paid). The user shall also seek to obtain compensation for the damages from the supplier to the extent that they are the responsibility of the supplier.

The example that comes to mind is a company that has to suspend its activities due to a failure in the operation of a computer application. In such case, if the company suffers losses (unrealised business, salaries paid to employees that cannot work, etc.), it may seek to demand indemnification by the supplier.

To consider the supplier to be liable for the damages, the fault or defect causing them must not have been fortuitous or the exclusive fault of the user itself, but rather must be attributable by some means to the supplier-licensor:

- Either for what is legally known as **wilful misconduct**: when the supplier was aware of the existence of the malfunction or defect in the software that caused the damages to the user.
- Or for fault or **negligence**: when the supplier was unaware of the existence of the malfunction or defect but should have known, had they performed their duties of programming or maintenance of the software with the degree of diligence expected from any programmer.

In addition, liability can arise for a variety of types of damages, direct or indirect. As with warranties, software licences tend to reference the types of damage contained in the law of English-speaking countries. Generally speaking:

- **Direct or incidental damages**: those that are the direct result of the incident (for example, again, the loss of information or the expenses for the reconstruction of the lost information).
- **Indirect or consequential damages**: those indirectly derived from the incident, whether the parties knew or should have known that they could

have been sustained in the event that such incident were to occur (for instance, loss of reputation with clients).

- **Lost profits**: There are certain damages, such as the loss of profits, which would in principle be included as indirect damages. Nonetheless, on occasions, the criteria of the British and United States courts have varied, including them sometimes as direct damages. Therefore, licences tend to cite loss of profits separately.

As regards Spanish law, for example, the following are defined:

- Consequential damages: the value of the various equity and moral losses directly sustained by the user as a result of the incident (for instance, if a software malfunction causes a loss of information, the value of such lost information; or damage to the image that an entrepreneur user sustains with respect to clients), and the expenses incurred to remedy such incident.
- Lost profits: profits not obtained by reason of the incident (for instance, the income that the entrepreneur user does not receive during the time in which their activity is suspended due to the software malfunction).

1.7.4.　Limitations and exclusions of warranties and liabilities

Suppliers tend to include warranty and liability limitation and disclaimer clauses in software licences. Although the principles of law generally allow for contractual freedom (in determining the contracting conditions) the legal effectiveness of such clauses is questionable.

Warranty disclaimers

Software suppliers-licensors seek to avoid certain warranties that they should provide the user or to shorten the term for which they should be provided, imposing warranty limitations or disclaimers for such reason in the text of usage licences. Should the licensee consumer have agreed to the licence agreement without negotiation, under the laws for the consumer and user protection these limitations could be declared null and void and be left out of the agreement for being abusive. Therefore, the minimum legal warranties that we just described cannot be limited in such circumstances.

Nonetheless, if the licensee is not a consumer but a business or professional, the supplier may be entitled to restrict its warranties and liabilities in the licence. Nonetheless, they cannot shirk any incidents occurring to the software quite so easily and the licensee could resort to the analogous application of the (Civil or Commercial Code) rules providing for a warranty of repair of hidden defects, applying the principle of good faith in agreements and others, to demand that the supplier should ensure that the software should remain in perfect state of operation. The validity or absence thereof in limitations of warranties must be determined on a case-by-case basis.

Liability limitation and disclaimer

Additionally, software licences typically include clauses of disclaimer of the liability of the supplier with respect to damages sustained by the user due to incidents with the software. Or, if indemnification is due to the user for damages, they limit the possible indemnification of the supplier: for instance, it is common to limit it to an amount equivalent to the price that the user has paid for the licence (along with the payments made for maintenance services).

In many cases, the validity of these liability disclaimers or limitations is dubious at best. What can be said with certainty is that the liability disclaimer or limitation shall not be valid when:

- The liability derives from wilful misconduct: wilful misconduct not only occurs when the supplier causes the damage knowingly (which would not be very normal), but also when the supplier knows of the existence of an incident that could cause certain damage to the user and does nothing to prevent the damages.

  Gross negligence. In countries other than Spain, just as wilful misconduct, liability for gross negligence cannot be subject to limitation: when the incident is attributable to the supplier, due to a lack of the diligence expected from any supplier.

- Liability for damages consisting of the death or corporeal damages to people: in principle, we find it hard to think of a program whose malfunctions or errors could cause such damages, except in certain specific cases such as the software of a medical device, applications used by air traffic controllers, etc.

- When the licensee suffering the damages is a consumer: under the provisions of the Consumer Protection Law, consumer users are entitled to compensation for the damages sustained as a result of the malfunctions or unsuitability of the software, unless these are their own exclusive fault. Therefore, if the licensee is a consumer, the supplier cannot validly reduce the liability limitation to a maximum amount, as such a clause would automatically be null and void for infringing upon the law and for being abusive. Nonetheless, when the user-licensee is a business or a professional, the liability limitation to a maximum amount is valid in principle, as the legislation allows the parties to agree on this issue.

  This is important as suppliers are especially interested in limiting their liabilities with respect to licensees that are businesses or professionals, as software malfunction could imply for them damages of much greater importance –at least in economic terms – than with a consumer.

  Notwithstanding the foregoing, even if the user-licensee were a business or a professional, it would be necessary to study each specific case to determine whether the limitation of liability could be especially unfair and abusive. In such case, the limitation could be declared null and void, if it were considered that the limitation of liability is so disproportionately abusive that:

- in practice, it implies making the supplier totally irresponsible for its own obligations; and/or
- it breaches the principle of good faith in agreements.

In the UK, case law generally has established that when the licensee is a business or professional, the supplier-licensor may limit its responsibility under the licence when doing so is not "unreasonable". To determine whether liability disclaimer or limitation is reasonable, the courts take into consideration various circumstances, known as the reasonableness test:

- Whether there has been a true process of negotiation of contractual clauses, particularly those relating to warranties and liabilities. Or whether it was the opposite and the supplier imposed the content on the licensee.
- Whether the licensee knew of the existence and scope of the limitation clause, whether they were under advice from counsel to inform them in that sense before signing the licence.
- Whether the limitation or disclaimer clause was accepted by the licensee in exchange for something in their favour (for instance, a price reduction).

1.7.5. Warranties and liability in free software licences

It is said, and it is true to a great extent, that free software licences are granted with no warranty whatsoever for the user and that no sort of liability is assumed. This is debatable, especially in the legal framework of European and Member State laws, especially those seeking full exoneration of liability.

GPLv3

"there is no warranty for the program, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide the program "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the program is with you. Should the program prove defective, you assume the cost of all necessary servicing, repair or correction".

Governing law and the facts of the case will ultimately determine whether the supplier of free software should provide a warranty or whether they incur any liability with respect to the user-licensee.

The validity of such absence of warranties could be upheld when the free software is distributed free of charge and the limitation of liability is subject to "the extent permitted by applicable law". Indeed, it could be said that the distribution of free software may be equated to a gift. And the rules governing gifts generally do not compel the giver (in this case, the supplier) to provide warranties regarding the gift (in this case, the right to use the software) with respect to hidden defects or to insure its proper operation. If the gifted item proves defective, the giver usually has no obligation, in principle, to repair it or substitute it with another. The liability would be different in the indemnification of damages sustained based on a malfunctioning or defect.

In any case, we must take into consideration that not all free software is entirely "free". When the licence for free software is granted accompanied with the supply of additional services, such as maintenance or update services (the case of "Red Hat" for instance), the supplier charges to provide such services. It

must therefore comply with obligations with respect to the proper rendering of the services (proper choice of a free software solution, good adaptation and implementation for the user, etc.).

There is also the question of whether it is the licensor himself who should provide the warranties (certainly as to title), or the person who supplied the software (probably as to quality and fitness).

With respect to limitations of liability, the question of the validity of the clauses is more doubtful:

GPlv3, Cl.16

"In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who modifies and/or conveys the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages."

Regarding this liability disclaimer, there would not seem to be many circumstances –as regards free software– that would allow the supplier to disavow the applicable legal system, which prohibits absolute liability disclaimers. Furthermore, as we have already seen, there can be no disclaimer or limitation of liability, when derived from wilful misconduct or if the licensee were a consumer. In other words, this clause would be ineffective with respect to a licensee consumer.

The Free Software Foundation itself and other entities developing free software projects are aware that some warranty and liability disclaimer clauses, in absolute terms (as is), have validity issues in many countries. In this sense, warranty and liability disclaimers tend to include a typical mention that such exonerations are valid "except as required by applicable law" or "to the extent permitted by law".

Version 3 of the GNU-GPL has complemented the qualification with its clause 17, destined for interpreting the warranty and liability disclaimers established in Clauses 15 and 16: "If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the program, unless a warranty or assumption of liability accompanies a copy of the program in return for a fee".

Beyond the legal effectiveness of the warranty and liability disclaimer clauses, free software licences tend to provide that a licensor may choose to voluntarily provide some type of warranty for the software or assume some degree of liability, in principle in exchange for an economic consideration (for instance, under the framework of the rendering of maintenance services).

An important aspect is that, in these cases, the licensor of the free software assuming warranty or liability commitments with the users, does so personally and does not thereby bind prior licensors of that same software, from whom the free licence was acquired.

Other free software licences establish similar provisions, such as the Apache 2.0 licence (clause 9), for instance.

1.8. Jurisdiction and applicable law

Many software licences expressly establish a clause regarding competent juris-
diction and governing law, which is of great importance in case of conflicts
between the parties leading to litigation. These clauses are especially relevant,
obviously, when the supplier and licensee reside in different countries.

Under such agreement, the licence determines:

- **Jurisdiction**: the courts of the country (region, city, etc.) that shall have
  competent jurisdiction to resolve upon any litigation between the parties
  derived from the licence. Therefore, if one party wants to claim something
  from the other, it must do so before the courts agreed to have competent
  jurisdiction.
- **Applicable law**. The law (laws, regulations, etc.) of the country should
  govern in applying and interpreting the clauses of the licences. In case of
  litigation, the court or arbitrator designated as having competent jurisdic-
  tion must resolve upon the matter in accordance with the law agreed by
  the parties to be applicable.

Should the parties not have expressly agreed upon the competent jurisdiction
and/or law applicable to the licence, it would be necessary to abide by what
is determined in the norms on "Conflict of Laws[8]" of each country.

[8]The area of Conflict of Laws, or Private International Law, is extraordinarily compli-
cated, and even more so in the realm of intangible transfers, downloads, content man-
agement systems and worldwide audiences, web-services and software as a service.

For the purposes of this section, it is sufficient to know that, in principle,
agreements reached between business parties establishing competent jurisdic-
tion and the law applicable to the agreement in the licence are valid.

An exception exists, once again, when the user-licensee is a consumer. In such
case, the user may sue the licensor both in the courts corresponding to the
domicile of the licensor and those of its own domicile (which would undoubt-
edly be more convenient and economical for the user). On the other hand, if
the licensor seeks to sue the user, it may solely do so before the courts of the
domicile of the consumer.

Even if an applicable law other than that of the country of residence of the
user is agreed, the user may regardless seek the application of the consumer
protection laws of their country of residence.

Consider a software licence in which the supplier is from the United States and the user
is a French consumer. If, for instance, the licence establishes that the competent courts
are those of the United States and the applicable law is that of the Federal Law of the
United States and the Law of the State of California:

- The user could also sue the supplier in France and the French courts would be deemed
  to have competent jurisdiction.

- The user could invoke the application of the Consumer Protection Law and other norms protecting consumers in French.

However, for licensee consumers to be able to benefit from these norms that protect their interests, they must have contracted the licence with the supplier, who must have engaged in any sort of commercial activity specifically directed to the country of residence of the user (advertising, opening of a store, etc.).

This is important considering the numerous licences contracted over the internet, particularly on the websites of software suppliers. In principle, in case of litigation for a software licence acquired over the internet, the user consumer could only benefit from the aforesaid protective norms if the website is directed specifically to their country of residence (either in conjunction with other countries or on its own).

Continuing with the last example, let's assume that the licence corresponds to software downloaded off the internet. It would be necessary to verify whether the website of the United States supplier is by any means specifically directed to France (for instance, through such expressive signs as having a section in French, showing a price in Euros or indicating technical service or a branch of the supplier in France). It would be in such a scenario that the licensee consumer could sue the supplier in France, in the event that a dispute was to arise between them, and require the application of French consumer protection regulations.

2. Software contracts

Most software is not created by an independent programmer for his/her own exclusive use or that of few people. It is created by companies that precisely develop and distribute software for third parties that they trust has uses and applications that will satisfy the expectations and needs of determined users. In this section, we comment on the licensing issues relevant to certain business models.

A software licence adapts to all types of software, both "standard" (for an indeterminate amount of users), and "customised" (commissioned by a client), and "parameterised" software mentioned below. In each case, the original software owner (and the owner of the modifications or parameterisations) must grant user rights to the user. The difference lies in that for "standard software", a "standard" user licence is used (the EULA of Microsoft Windows or the GPL), while for "customised" or "parameterised" software there tends to be negotiation between the parties in terms of the legal user conditions.

2.1. Standard mass market software

The purpose of companies developing mass market or "standard" software (usually without adaptations to the particular needs of the user) is to distribute software among the largest number of users possible to obtain its utmost dissemination and, why not, the highest economic benefits. It is said, for that reason, that this software is "mass" traded or distributed.

Often standard software serves to cover more than the needs of the users acquiring it – think of all the macro functions of word processor software that the everyday user doesn't even know about, let alone use. Users, in turn, find it much more economical to purchase a standard software licence than to commission a programmer to make them a "customised" word processor, for instance.

In the case of "traditional" non-free software, the income is greater the more copies of the program are sold. Licences are drafted to prevent reproduction and redistribution of the software, which would eliminate revenue, and also prevent modification, which could give rise to malfunctioning and difficulties to provide user support and maintenance services (patches, etc.).

Example

E.g.: Symantec Product License agreements.

2.2. "Bespoke" software

When a programmer or a programming company creates (unique) new software on commission from a client, adapted to its needs, and which must satisfy the instructions and exclusive needs of such client, the result is called bespoke software.

The contractual relation between the two parties is governed by a "software development agreement", which governs specifications, delivery, acceptance, guarantees, price, etc.

One of the most important clauses of a software development agreement is the ownership or "title" clause and copyright licence, determining who is to own the software created by the programmer and what are the exploitation rights.

- Title may be attributed to the client ("*work for hire*" model, in the USA). In this case, the programmer (author of the software) assigns the exploitation rights to the client.
- Title may remain with the developer. In this case, for the client to be able to use the software, the development agreement provides that the programmer grants the client a user licence.

The developer may also maintain control over certain parts of the bespoke software that are used "generically" in their developments (licensing it to the client) and assign the exploitation rights to the part that is truly "customised" for the client.

2.3. Customised software

Additionally, in many enterprise situations, adaptations may be made to a standard application, such as Enterprise Resource Planning software (ERP), Document Management Systems (DMS) or Content Management Systems (CMS), according to the particular needs of each client. The adaptations are often called customisations or parameter changes ("parameterisations", also known as "extensions"). This is more in the line of a service agreement, with the client taking a licence from the manufacturer of the standard application, and hiring the services of the developer for the customisation and deployment.

In these circumstances, although the application software may be non-free, the fact that the solution incorporates adaptations conforming to the needs of the user may also imply that the user-licensee may have a limited right to modify the software and access the source code; specifically, to create, modify or remove the customisations or parameterisations.

In the cases of both bespoke and adapted software, the project may be described as "turnkey", whereby everything is supplied to the client in an immediately working condition. In these agreements, not only is a user right granted to the user for the software, but also a warranty or specific result in their favour is expressly agreed, i.e., the software satisfies the specific needs of the user-licensee. A "turnkey" licence may, in principle, apply to either non-free or free software.

2.4. "Mass" contracting and general conditions

As seen before, the software licence is an agreement between two parties. Nonetheless, almost always one of them (the software supplier or licensor) unilaterally establishes the terms and conditions of the licence. In such case, the user cannot negotiate the licence conditions with the licensor, but must merely accept or reject them. This is a logical consequence when dealing with standard software, destined for "mass" distribution, whether or not it is intended to obtain an economic benefit.

The software supplier clearly cannot and does not want to negotiate the terms of the licence with each of the hundreds or thousands of users. Rather, on the contrary, the supplier wants all of them to use the software in accordance with the same conditions imposed thereby. Clearly, if the user does not accept the conditions, they do not acquire the licence and, accordingly, cannot use the software.

When a software supplier imposes upon all users the same terms and conditions of the software licence, which they may only accept (if they wish to use the software) or reject, we are dealing with an "adhesion agreement" and it is said to be based on general conditions.

> On some occasions, licences also have particular conditions, applied solely to a specific contractual relation: for instance, if the licence contains any clause regarding the adaptation (customisation) or "parameterisation" to the specific needs that a particular user has indicated to the supplier.

The use of general conditions is subject to the meeting of certain legal requirements. In the European Union, laws apply regarding the general contract conditions seeking to protect the position of the contracting party "acceding" to the conditions in the event of abuses by the entrepreneur or professional imposing them.

> The main requirements are usually that:
>
> - The general conditions must be drafted precisely, clearly and simply.
> - The acceding party must have been allowed to go over them before accepting the agreement.
> - The party imposing them cannot benefit from an unclear or ambiguous wording: in case of doubt in terms of its interpretation, the clause shall be construed in a sense favouring the acceding party.
> - If a general condition has a content that is incompatible with a particular condition, the particular condition shall prevail.

- Furthermore, if the acceding party is a consumer, as we have seen, some clauses are considered abusive and cannot be imposed, as they are considered unfair and disproportionately unfavourable for the consumer.

These will in fact also apply to free software licences, though it would be difficult in any circumstances to argue that the terms of the licence are abusive, given the extent of the rights that are granted, the few limitations, and the non-cost free nature of the software, in most circumstances. What could fall under scrutiny are the limitations on warranties and liability, which are likely to fall foul of consumer protection based legislation.

2.5. Agreements ancillary to the software licence

Along with software licences of a certain complexity, directed to companies, there can be certain additional service agreements, which we shall refer to as "ancillary agreements" to the software licence, as their existence is dependent on the software licence to which they are associated.

These agreements may be contained in a document separate from the user licence, but may also form part of the licence agreement, whether incorporated among its clauses or as an attachment thereto. Among the most noteworthy of such ancillary agreements are maintenance agreements and consulting and training agreements (which are sometimes combined with the former).

Maintenance agreements

Software operation is relatively unstable and its possible malfunctions are not easy to repair, especially if the user does not have the source code. It also becomes obsolete quite quickly. Therefore, once the warranty period offered by the supplier for the software with the licence has ended, it may be essential for the user to maintain the software, especially the software of some complexity, destined for businesses and professionals. For the software supplier, providing the maintenance service will imply a complementary, and even a quite important, source of revenues. Providing a maintenance service also allows improving the software and repairing any faults advised by the users.

Through the maintenance agreement, the service provider undertakes to the user to maintain the proper operation of the software and/or to provide successive new versions, in exchange for a maintenance fee (annual, quarterly, monthly, etc.).

> In the case of non-free software, the maintenance service may often solely be provided by the software supplier or someone authorised by the supplier: they are the only ones with the source code and the only ones with the right to modify the licensed software. Users may be "captive" of the software manufacturer or service provider.

With free software, the business model may be based on providing such services as maintenance, but in this case, for a different reason. It is not a matter of more income for the software owner (the income for granting the licence is nil or minimal), but as there are no exclusive rights to the software, the

maintenance services are provided in free competition. Software integrators and consultants may compete among each either to provide a better, cheaper or more reliable maintenance service.

> With FOSS, anyone with the appropriate expertise could provide this type of service, enabling users to shop around and change support provider. Many professional or enterprise free software projects, such as Red Hat, Alfresco, Pentaho, etc., use this type of agreement as a significant revenue stream in relation to the licensing of their free software.

Service modes: there are typically three forms of maintenance service. Many agreements establish several or all of these modalities:

- Corrective maintenance: technical assistance to correct the errors or malfunctions in the operation of the software.
- Preventive maintenance: technical assistance through regular reviews, for instance, to avoid errors from occurring during operation.
- Development or update maintenance: consisting of providing the user with the improvements or new versions successively launched to market by the supplier.

Consulting and training agreements

Software suppliers often provide a service to users that consist of attending to inquiries relating to the selection, integration, installation and operation of the software. This is distinguished from the maintenance agreement in that, in this case, the purpose is not to avoid or correct issues with the software, but to create a solution for the needs of the user and to resolve any doubts relating to its operation for the user.

Being a service that users need, especially at the beginning of their use of the software when they are still not well acquainted with it, this service could possibly be included with the licence as ancillary to the subsequent installation of the program.

As part of the consultancy agreement, a possible variation lies in training: when the technicians of the supplier teach the employees of the user how to operate the software or teach courses on its use.

As for maintenance agreements, in the case of free software, the consulting and training service may be rendered in circumstances of free competition by any computer services company, as access to the source code of the program is open and anyone can gain sufficient skills to install, develop and train clients on the software.

3. Free software and free content

We have seen in the introduction to this module that the free software and content movement (including for these purposes, the open source and the free content movement) has positioned itself as the defendant of access to and dissemination of certain forms of culture and knowledge in an increasingly restrictive society, where IP laws are used to control the exploitation of works to an ever greater extent, in the face of technological change.

The focus of this section therefore is to understand the basic concepts of the free software and content movement, before looking in more detail at free software and content licences.

3.1. Free software

Although a precedent exists at the University of Berkeley and in the BSD licence that we shall comment on below, for many the founders of the free software movement, round 1983-1984, were Richard Stallman and the Free Software Foundation. Richard Stallman, who at the time was employed at the MIT AI Lab, abandoned his work to undertake the GNU ('GNU is Not Unix') project and founded the Free Software Foundation to obtain funds and a more formal structure for the development and protection of free software.

> Richard Stallman established the ethical foundation for free software in such documents as "The GNU Manifesto" and "Why Software Should Not Have Owners". Since the beginning of the GNU project, Richard Stallman was concerned with the liberties that would be available to the users of the software created. He is interested in that, not only those receiving the programs directly from the GNU project, but also those receiving them following any number of redistributions, could continue to enjoy the same rights (modification, redistribution, etc.).

The basic tenets of the free software movement is the need to ensure that users of software have significant freedom (in legal terms, rights) to exploit software, understand it, learn from and it share it with third parties.

The Free Software Foundation established a core definition for free software: software under a licence that allows and guarantees the exercise of the following four freedoms to the users:

• The freedom to run and use the software for any purpose (freedom 0).
• The freedom to study the program and adapt it to your needs (freedom 1).
• The freedom to distribute copies (freedom 2).
• The freedom to modify the program and release the modifications to the public (freedom 3).

> See online at the GNU site. The importance of this definition is twofold. On the one hand, the free and open source community is in agreement with it and respects it; even thought different parts of the community may have differing philosophies or views. On

the other hand, from a legal perspective, it is a unifying tool for the analysis of free software licences: it separates what is free from what is not.

To enjoy such freedoms, especially 1 and 3, the user must have access to the source code of the program. Free software licences indeed contain a commitment by the supplier-licensor to provide the source code to users or, at least, to make it available to them. Below we shall briefly analyse how the users are granted the rights of use, copy, modification and distribution in free software licences.

> In English, the word free has two meanings: 'unencumbered' and 'without charge'. It should therefore be clarified at this time that the use of the term "free" in relation to software does not imply that the owner or provider of the software provides or distributes it free of charge (although they may). The term free refers to the software being distributed under a licence that allows users to use it freely. As regards the economic consideration for the distribution of free software, we shall see that most licences allow the distributor to use the price of their choice.

> The BSD free software licences allows code to be privatised or "closed" and, therefore, its sale as a commercial product. The General Public License (GPL) explicitly allows charging for distribution (clause 1). The price is solely limited by the rule of market: as the user could subsequently publish the source code on the internet or by any means distribute it free of charge, any third party could obtain a copy without paying.

Why not public domain?

Without doubt, the simplest way to make a program free is to make it an object of public domain, with no rights reserved. This allows the creator to share the program and its improvements with the entire world with no restrictions. But this solution will allow third parties to use the software in a manner that may go against its original philosophy, making it non-free or closed software. To avoid such a possibility, the FSF created the concept of *copyleft* and protected the GNU and software against future intermediaries that could attempt to restrict the freedom of the users to redistribute and change it.

> Additionally, as we have studied, in continental systems, moral rights are inalienable, which means that it is also impossible to voluntarily place software under public domain, waiving the moral rights thereupon. Nonetheless, even in English-speaking countries (where the figure of "moral rights" does not exist as applied to software and software may indeed be placed voluntarily under public domain), which is where free software licences originate from, it has also been sought to clearly provide that the original author of the free software does not waive their status as such. Therefore, it is common among the various modalities of free licences to maintain a notice of authorship.

3.2. Copyleft

Thus, if free software rights are granted unconditionally, a user would be free to incorporate the software and any work resulting from using the software into a proprietary or non-free program. According to the supporters of this movement, for the free software philosophy to be truly effective, derivative versions must also be free. The goal of "*copyleft*" is to establish a licensing framework whereby the essential freedoms are granted but free software may not

be transformed into non-free or closed software. Copyleft guarantees that all derivative work, based on the free software distributed with copyleft, shall be available under the same free terms.

Copyleft may thus be defined as a manner of licensing rights in a work with the particular condition obliging redistribution of the work, and any derivative work, to be on terms that maintain the freedoms of use, modification and distribution for all future users and licensees: no further restrictions may be added.

To accomplish this objective, R. Stallman wrote the General Public License (GPL) as a foundation to guarantee the freedom of all free software users at all times. Thus the GPL goes beyond guaranteeing the four basic freedoms, and includes terms compelling the use of the same licence (the GPL) when redistributing both the original software and any work derived from it (and potentially any other work including it) and offering access to the source code. In other words,

• Redistributors are not allowed to add additional restrictions to the licence (other than those of the original GPL).
• In general, they must accompany any binary code with the relevant source code.

This mechanism is also used in other licences, including the Lesser GPL (LGPL), the Mozilla Public License (MPL), the Common Public License (CPL) and the Open Source License (OSL), discussed below. Most of these are characterised by a "weak" copyleft, as they solely affect the original software (and the derivative works), and not the works using or containing the software with such licences.

However, the GPL is important not only because it is the most used licence in the free software world (accounting for 70% of the free projects on Sourceforge) or because it is the precursor of many other current free licences (not all of them, though, as the BSD predates it), but because the principle of freedom of the FSF has been the basis and one of the most outstanding elements of the free movement.

On the basis of this copyleft condition, the pool of software subject to copyleft available to all may only increase as new applications are created by developers based on the software distributed under a copyleft licence.

The term copyleft is based on a play on words: copyleft uses copyright laws and legal framework, which is basically restrictive, but turns them around to serve the opposite of their usual purpose. Rather than being a means of keeping software private or undisclosed, it becomes a means of keeping it free. The developers of non-free software use copyrights to restrict the freedom of the users and to restrict its free reproduction; the GNU movement uses the reserved rights to guarantee their freedom and that is why they reversed the name.

This copyleft concept has had phenomenal success in the sector and the FSF is the institution *par excellence* defending the values and ethics of the free software movement. In 2006-2007, the FSF reconsidered the GPL, then in its 2nd version, in the light of the technological and legal changes, and presented to the community a draft of a new version of the GPL (GPLv3). The process of drafting of the new licence, up until its final approval in June 2007, was

complicated and protracted and stakeholders were as varied as multinational companies, the academic sector, the individual developers and the public administration.

> The specific implementation of copyleft used for most GNU software is the GNU General Public License, or GNU GPL for short, and the GFDL for GNU manuals (using a copyleft adapted to documents). There is also the GNU Lesser General Public License (GNU LGPL), which is applied to some GNU libraries. Other copyleft licences (of various types) include the Open Source License, the Common Public License, the Mozilla Public License, and others that we will comment on below.

We stress that the Free Software movement by the FSF is essentially a philosophical, ethical and political movement. It is not a technological organisation or free software project (that would be the GNU project, the project closest to the FSF).

It should also be noted that copyleft does not affect the rights of use of the original licensee (an end-user, for instance), but restricts the freedoms relating to the subsequent distribution of the copyleft software with or without modifications (or closely incorporated in other applications). To understand this allows understanding why a copyleft clause does not affect the commercial use of applications subject to copyleft at private or public organisations, as such organisations are normally end users.

It is also necessary to stress that the legal impact of the copyleft clauses has led to great concern in the software world in general. It has especially been feared that the interrelation or incorporation of code with the GPL in other programs could affect the use or distribution of the resulting application or that the use of software with the GPL (for instance GNU/Linux) could prevent the use of other non-free applications. These doubts, which are often myths, are addressed below.

3.3. The Open Source Initiative and open source software

In 1998, there was a certain conceptual difference of opinions in the free software movement that in truth merely brought to a head the division that had been seen since the early nineties. This division gave way to the creation of the Open Source Initiative (OSI), which established the open source definition to determine whether a licence was "open source" or not (OSD).

> For some, the term open source is a modality of free software; for others, it is a general term that encompasses all free software and, finally, for others, it is a dangerous departure from the original concepts of free software to achieve enhanced commercialisation.
>
> The Open Source project was born from a strategic meeting held in February 1998 in Palo Alto, California, to react to the plan hatched by Netscape Inc. to release the source code for its browser, the Netscape Navigator. Among the present were Eric Raymond, Bruce Perens (then leader of the Debian group), John "Maddog" Hall (from Linux International) and Sam Ockman (representative of the group of Linux users from Silicon Valley).
>
> See "Open Sources: Voices from the Open Source Revolution" (O'Reilly, 1999).

The OSI seeks to reconcile the freedoms of free software (in general) with the commercial needs of the companies involved in the creation, distribution and use of free software. By doing so, open code software maintains the fundamental freedoms of the free movement (reproduction, transformation, distribution, access to source code), but not the name "free software". It is replaced with "*open source software*", as the OSI considers that the excessive emphasis made by the FSF on moral or ethical reasons for the freedom of software could cause negative reactions on the business mentality and that it is more beneficial to promote free software on its technical merits.

> On the other hand, note that the FSF does not agree with the use of the term open source to refer to free software, precisely as it makes it lose the ethical dimension referring to freedom. See "Why Open Source misses the point of Free Software", R Stallman.

As a result of this initiative, the Open Source Definition was established. The OSD was designed to establish an open and understandable statement of the principles of the free software movement and a system for the classification and "certification" of the variety of free licences in existence. It is argued that, by establishing standards in this manner, the definition allows developers, users, commercial organisations and the public administration to better understand the free software movement and better respect its principles.

> It should be noted that open licences are free licences and vice versa. The difference between the OSI and the FSF (as institutions) is in their perspective (marketing, underlying philosophy, etc.) and not their principles in relation to licensing, which are shared by the two entities. In truth, the differences are not legal, but of position –the OSI stressing more the need to access the source code and the FSF placing more importance on the ethics or philosophy of "freedom". It is clear that the GPLv2 and the GPLv3 are "open" licences, conforming to the OSD: they are OSI certified.

The Open Source Definition (OSD)

The OSD was born from the *Debian Free Software Guidelines* (DFSG), revised in 1998, basically to eliminate references to Debian. The definition of open source software in the DFSG was indeed broad enough to include such licences as the BSD, the GPL and its sister the LGPL, and such others as the MIT/X and the Apache. Its requirements were therefore adopted by the OSI as general guidelines to be met by all open licences.

The definition of the OSI stresses the four fundamental elements of the free software movement, expressed in the four freedoms listed by the FSF. Additionally, availability and access to the source code is fundamental: the word *open* could be better translated by *'available', 'visible'* or *'readable'* and we could speak of *available* source code software licences.

The Open Source Definition

Introduction

Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution

The licence shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The licence shall not require a royalty or other fee for such sale.

2. Source Code

The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicised means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3. Derived Works

The licence must allow modifications and derived works, and must allow them to be distributed under the same terms as the licence of the original software.

4. Integrity of The Author's Source Code

The licence may restrict source-code from being distributed in modified form only if the licence allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The licence must explicitly permit distribution of software built from modified source code. The licence may require derived works to carry a different name or version number from the original software.

5. No Discrimination Against Persons or Groups

The licence must not discriminate against any person or group of persons.

6. No Discrimination Against Fields of Endeavor

The licence must not restrict anyone from making use of the program in a specific field of endeavour. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of Licence

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional licence by those parties.

8. Licence Must Not Be Specific to a Product

The rights attached to the program must not depend on it being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's licence, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. Licence Must Not Restrict Other Software

The licence must not place restrictions on other software that is distributed along with the licensed software. For example, the licence must not insist that all other programs distributed on the same medium must be open-source software.

10. Licence Must Be Technology-Neutral

No provision of the licence may be predicated on any individual technology or style of interface.

Example

An interesting example of the OSD application is seen in the case of KDE, Qt and Troll tech. KDE is a desktop graphic interface for Linux and depends on graphic libraries called Qt, owned by Troll Tech. Nonetheless, the Qt licence did not conform to the OSD, as a special licence was required to incorporate such libraries in applications that were not X Windows System. (Qt obtained income for the assignment of licences to Microsoft and Apple). Therefore, the free application KDE incorporated elements that were considered not to be free. Under pressure from the free community and the OSI in particular, Troll Tech agreed, initially, to create a special licence to release the Qt code in the event of the merger or bankruptcy of the company. Later, at the beginning of the development of GNOME, an open product competing directly with KDE, and with the creation of free libraries similar to Qt (such as Harmony), Troll Tech modified its licence to conform to the OSD.

It was argued that by establishing standards in this manner, the definition would allow developers, users, commercial organisations and the public administration to better understand the free software movement, enhance respect for its principles and, why not, find new business models to guarantee their future.

The OSI has further prepared a certification mark, the OSI Certified, which is a clear means of indicating that a licence complies with the OSD. The mark also serves to distinguish the term general open source, which has not had a sufficiently-defined use to guarantee such conformity.

3.4. Free software licences

Both the FSF and the OSI implement their philosophy and strategy through a work tool of legal nature: a free software licence. The FSF, by publishing the GPL and LGPL, and now the Affero GPL (AGPL, specifically designed for software distributed as a service or the offering of remote software services). The OSI, due to the cataloguing and classification of the various free licences used more or less by the community, published on its website: www.opensource.org.

As seen earlier, the difference between free software and non-free software lies in the rights and obligations specified in the licence. Those granted under free software licences offer a broad freedom to exploit the software, in terms of its use, modification and distribution, and tend to be directly opposite to those granted and reserved by a non-free software licence ("non-free licence").

We should recall that the four freedoms correspond to exclusive exploitation rights reserved to the owners of author's rights by applicable law:

- Freedom 0: the use right (not an exclusive right, but the free licence allows unrestricted and indiscriminate use).
- Freedom 1: the right of modification.
- Freedom 2: the rights of reproduction and distribution.
- Freedom 3: the rights of transformation and distribution of derived works.

All free software licences must therefore license these rights to users.

> For instance, the MIT licence establishes that "permission is hereby granted [...] to any person obtaining a copy of this software [...] to deal in the software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-licence, and/or sell copies of the software [...]", while the BSD licence provides that "redistribution and use in source and binary forms, with or without modification, are permitted [...]".

It is important to understand that not all free software licences are the same. The range of possibilities span from some minimum requirements (e.g. the BSD and MIT licence), solely requiring the maintaining of the copyright notice and warranty and liability disclaimers, up to the "maximum" (in certain sense) of the copyleft clause of the GPL, requiring the user to distribute any modifications and derivative work under the same GPL.

> As a result of the obligation to freely distribute any modified or derivative work, it has been said that "the GPL is not as free" as other free licences. The FSF rejects such classification arguing that, quite the opposite, the GPL is freer, as it guarantees greater freedom for the end user. Consider the following:
>
> - The BSD, for instance, grants the developers more freedom, as they may incorporate and distribute implementations of "BSD codes" under both types of licences, free and non-free.
> - The GPL gives the end users greater freedom as they always receive applications with open source code and a free licence.

Briefly, free licences may be classified into three categories: permissive licences, free licences with strong copyleft and free licences with weak copyleft.

- **Permissive (or "academic") free licences.** The Berkeley Software Distribution (BSD) licence is perhaps the simplest version of all free licences, and is also the first free licence ever created. It grants full exploitation rights and solely requires maintaining copyright notices and disclaimers of guarantees and responsibilities. It is a result of the distributions of versions of Unix by the University of California, Berkeley, in the seventies and eighties. The philosophy behind this licence is that the code is the fruit of the research and work of the University, financed by the Government of the United States (and the taxes of the American people). Therefore, it must be freely available and must protect what we refer to herein as the "moral rights" of the authors for the mere obligation to maintain copyright notices. The BSD has been the model for many similar licences, including the Apache licence and the licences of the X family (X, XFree86, XOpen, X11).

- **Free licences with strong copyleft.** The General Public License (GPL) is the most emblematic of the copyleft licences. Its purpose is to guarantee the four main freedoms of free software for all users and that any modifications be distributed under the same conditions. Others include the IBM Common Public License or the Sleepycat licence. They are known as strong copyleft licences as they do not allow their integration in major applications with other types of licences.

- **Free licences with weak copyleft.** These licences maintain the copyleft obligations for the core of the program distributed under the licence, but also allow their integration in works with other licences. The Mozilla Public License (MPL), the Lesser GPL (LGPL), the Open Source License (OSL) or the Common Development and Distribution License (CDDL) are examples.

Copyleft licences

GPLv2, GPLv3, AferroGPLv3, Sleepycat

Free licences with weak copyleft

MPL, CDDL, LGPL.

Free software rights

Looking at the rights that are granted under a free software licence:

- **Freedom of use**: The user of free software has full freedom to use and copy the software how, when, as much and where deemed convenient: install it on their hardware, store the necessary files and run it whenever they wish, in order to benefit from its applications. The user may use the software:
  – For any purpose or end. Therefore, the use of the software cannot be limited to the "personal use" of the user. Additionally, free software may be used for both private and professional purposes.
  – By anyone. Without there being room for discrimination due to the group of which they form part.

   – On any hardware devices deemed convenient, regardless of their technical characteristics.

- **Freedom to copy**: users of free software may make as many copies of the software as they wish, without being limited to solely copying the files necessary to run the software on their hardware, or to a single security copy. This freedom to copy is closely related to the freedoms of use (users may use the software on any hardware devices they wish) and of distribution (the user may provide copies of the software, with or without modifications, to third parties).

- **Freedom to transform, and access source code**: users also acquire the right to transform the licensed software: translate it, adapt it to their needs, debug it or combine it with other programs. To allow users to effectively use this freedom of modification, the supplier- licensor must furnish them with the source code for the software or, at least, make it available to them. As defined by the GNU-GPL and the OSD guidelines, source code is the "preferred form" for a developer to make modifications to the software. Conditions on the freedom of modification of free software. Generally speaking, most licences impose some conditions on transforming: they must respect the copyright notice of the original author and sometimes must indicate which files they have modified. The purpose of this condition is to protect the reputation of the original author facing the possible malfunctioning of the software based on a modification.

> **Supplementary content**
>
> GNU-GPL Version 3 states in its Clause 5.a) that the "the work must carry prominent notices stating that you modified it, and giving a relevant date".

- **Freedom of distribution and public communication**. Free software users have the right to distribute copies of the software with or without modifications to third parties, in tangible form or over the net. This is a very broad freedom, inasmuch as the user may distribute them free of charge or in exchange for economic compensation, temporarily (rental, loan...) or indefinitely; with or without source code (copyleft requires access to source code), verbatim or modified.

GNU-GPL Version 3, no longer uses the term "distribute", but the more generic term "convey" (convey literal copies of the source code, convey works based on the program, convey the program in object code with the commitment to make available the source code, etc.), to encompass what we understand in Europe to be distribution and public communication. Other free licences, such as the Apache 2.0, not only include the licence to distribute programs, original or derived, but also to publicly display them).

It is as to conditions on distribution that free software licences most vary. As we have mentioned, permissive BSD-type licences only require users to maintain the "copyright notice" and disclaimer when redistributing the software, both in source code and binary. Copyleft licences require redistribution of the work and derivative works to be done on the same terms as the original code. Strong copyleft extends this to works that are combined with or intimately interact with the original work. In some cases, the free software licences contain certain limitations to the redistribution of the software, when such redistribution may conflict with a patent: for

instance, the duty of indicating that the free software is being sued for the violation of third-party patents, identifying such third party (Mozilla licence).

3.5. Freedom applied to works that are not software

Free licensing was initially conceived to be applied to software, but it also may be applied to other types of works. Upon careful study of the GNU GPL, it may be seen that the licence may be applied to information other than software. The GNU GPL holds that "it applies to any program or work containing a notice placed by the owner of the rights, claiming that it can be distributed under the terms of the General Public License". In this sense, the "program" must not necessarily be a computer program. Work of any kind subject to copyright may also freely be subject to copyleft under the GNU GPL.

> The GNU GPL refers to the "source code" of the work; this "source code" implies different things for different types of information, but the definition of "source code" –as established by the GNU GPL– remains generic in any case: "the source code for the work represents the preferred form of making modifications to the work". However it sits awkwardly in relation to works other than software.

The FSF has further created a free licence for documentation, especially as the software is accompanied by technical documentation that is often necessary for its use. It would make no sense to distribute the free software without distributing the relevant documentation under similar terms. The General Free Document License was thus created to accompany their programs.

Creative Commons

The Creative Commons initiative (often abbreviated "CC") is a project created by experts in copyright law from Stanford University in the United States. Its purpose is to help authors and creators distribute their works for public use and thus extend the number of creative works available to all. It is especially directed to literary and artistic creations and not software, and expressly recommends the GFDL for any computer documentation and applications. The CC further provides a framework for dedicating works to the public domain, also under the conditions of the United States copyright laws.

Creative Commons is commented on in more detail below.

4. Free software licences

As mentioned earlier, the array of free licences spans from permissive licences, which impose no further obligations than that of attaching the conditions and the disclaimer, to licences with a strong copyleft, requiring that the same licence be maintained for redistributions of the software and of any derived work.

Along these lines, for the purposes of our study, we have classified free licences into three categories (plus one), to be examined in this section. These three categories are as follows:

- Permissive licences, BSD style, including MIT and X licences (compatible with GPLv2), and the AFL or ZPL (incompatible with GPLv2).
- Licences with strong copyleft: GPLv2 and GPLv3, in particular.
- Weak copyleft licences: LGPLv1 and the LGPLv2, the MPL and the OSL.

4.1. Permissive licences: no copyleft

In this section, we shall present some of the most commonly used free licences among the free development community, especially the BSD licence, which has served as the model for many other licences.

These licences are "at one end" of the array of free licences, as they do not contain copyleft obligations and allow for the privatisation of derived or collective works that include the software.

The first generation of these licences (BSD, MIT/X, Apache 1.0 and Apache 1.1) is characterised by being very short and not including any further obligations than those of maintaining the notices of authorship in the source files and the list of conditions (especially the disclaimer) when redistributing the software. The main objective of such licences is to grant the recipients full exploitation rights to the software (rights of reproduction, modification, distribution and public communication) so that the licensees may do "whatever they want" with the code. They do not contain copyleft and allow incorporating and combining the software with any sort of work, whether free or non-free. For instance, it is said that there are BSD software components in the Windows NT and Mac OS X operating systems.

The next generations (Apache 2.0 and AFL) include a series of new conditions relating to patents, governing law, etc., that are in line with the Mozilla Public License (which we shall discuss below), to modernise and clarify their terms.

Supplementary content
Most are born from the academic world (as indicated by their names: Berkeley Software Distribution, MIT, Education Community License...), and therefore they have been referred to as "academic licences".

4.1.1. Berkeley Software Distribution (BSD) and similar licences

The Berkeley Software Distribution (BSD) licence is perhaps the most simple of all free licences. It derives from the distribution of versions of Unix by the University of California, Berkeley, in the seventies and eighties, in the early beginning of the free software movement. The principle underlying the licence is that the software is the result of the college research and work financed by the Government of the United States (and the taxes of the American people) and that, therefore, it must be freely available. This means that it would only protect what we have referred to herein as the "moral rights" of the authors for the simple obligation of maintaining notices of authorship (copyright notice).

- Rights granted. The BSD allows unrestricted use, modification, copy and redistribution of software under the BSD, in object code (binary) or source code format.
- Obligations imposed. Distribution in form of source code is to be accompanied by a copyright notice, the list of conditions and the denial of any warranty and liability. Redistributions in binary code must reproduce the same things in the documentation. The name of the author and of the contributors may not be used for the promotion of derived works without their permission.
- Other terms. No warranty is granted in respect of the proper operation of the program and all liability is denied.

Therefore, almost anything can be done with codes under the BSD, provided the notice of authorship of the initial program is respected and the list of conditions is included in the code or documentation. It is also unnecessary to provide end users with the source code.

> The first version of the licence imposed the obligation to attribute each component to their original authors in any publication or promotional material of the program or derived work. This obligation implied certain hassles, as it was necessary to include extensive authorship throughout all the documentation and the source code, relating to each author adding their name to a licence. In a program with hundreds of contributors, this obligation was hard to meet. This also meant that BSD code was incompatible with GPL code. In July 1999, this obligation was stricken from the BSD licence. Regardless, at present, it is necessary to verify the version of the licence applied to BSD code, to make sure that it is not an earlier version and make sure that its terms are correctly followed.

The BSD-style licences allow for a great dissemination of the software and its use as a reference or standard (for protocols, services, libraries and even complete operating systems, such as Unix BSD). It nonetheless also allows what is known as code forking), inasmuch as anyone may adapt, modify and extend the program kernel and create a "similar but sufficiently different" version. This is seen, for instance, in the proliferation of operating systems with BSD-type licences, such as the OpenBSD, the FreeBSD and the NetBSD.

> Any software with a three-clause BSD licence (or new BSD) is compatible with GPL software (and almost any other free software licence), but not the other way around. In other words, BSD code may solely be incorporated in a GPL program (with the result of a work combined under the GPL), but GPL code cannot be incorporated in BSD software.

Other licences similar to the BSD

The BSD has been the model for many similar licences, among which we shall mention the MIT licences and those of the X family (X, XFree86, XOpen, X11), the Apache 1.1 licence (which we shall discuss below), Cryptix, Python, W3C Software Notice, Zope Public License (ZPL), LDAP Public License, Phorum, etc., and the OpenSSL and Sleepycat licences, which follow a simplified model of the BSD licence, but include copyleft clauses (as we shall discuss in the section on licences with copyleft).

The X and MIT licences are similar to the BSD licence but, on the one hand, they specify the permitted uses in further detail: "the use, copy, modification, merger, publication, distribution and/or sale of software"; and on the other, do not distinguish between distributions of source code and object code.

4.1.2. The Apache Software Licences (ASL)

The Apache web server project was created at the laboratories of the National Center for Supercomputing Applications at the University of Illinois, United States, and is now "run" by the Apache Foundation, in its technical and organisational, as well as its legal aspects.

The Foundation has drafted the Apache Software License (ASL), with versions ASL 1.0, ASL 1.1, and now, ASL 2.0, inasmuch as from January 2004 on, all software of the Apache Foundation will be published under ASL 2.0.

The ASL 1.1 is a variant of the BSD licence adding a few extra obligations:

- There is an obligation to maintain a notice with respect to the original authors in the documentation or redistributions of the software: "This product includes software developed by the Apache Software Foundation" (http://www.apache.org/)".
- Derived works should not use the Apache name without authorisation from the Apache Foundation (to maintain the reputation of the original authors).

Due to these additional obligations, the ASL 1.1 is not compatible with GPLv2. We should note that the first version of the licence (ASL 1.0) contained the same advertising obligation as the BSD with respect to the advertising materials mentioning the product.

The Apache 2.0 licence was published in January 2004 and belongs to a new generation of free licences. It is a very complete licence from a legal perspective, incorporating many of the modernisations contributed by the Mozilla Public License in 1998 (which we shall discuss in the following): complete

Supplementary content
Due to the importance that the Foundation and Apache software in general have in the free software community, in terms of software quality and its management model, the ASL is a licence that has been used by many other projects.

definitions, a patent licence and a patent peace agreement, an obligation to indicate modifications, a notice.txt file etc. It maintains its degree of permissiveness: it is not a copyleft licence.

- **Rights granted**. ASL 2.0 allows for the reproduction, modification, distribution and public communication (performance and display, under American law), with a right to sub-license, of the software under ASL in object code (binary) or source code format. Includes the explicit right to use another licence for the modifications or any derived work "as a whole", provided it meets the conditions of the ASL 2.0 licence.
- **Obligations imposed**. The redistribution of software should be accompanied by the licence, a notice if any files have been changed, any original notice of copyright, patent or trademark, any notice.txt file (with notices of authorship, modifications and any other legal notice). The name or trademarks of the licensor and contributors cannot be used.
- **Other terms**. No warranty is granted as to the proper operation of the program and all liability is repudiated. A patent licence is also included (revocable in case legal actions are brought based on patents against any other person with respect to the software).

Below, in the section dedicated to the Mozilla Public License, we will discuss the terms and objectives of the patent licence and the notice.txt file, as these concepts were created with this licence.

> As the Apache Foundation is a model for the management of free communities and projects, its new licence is an instrument used by many projects, especially those working with Java technologies or those of the Apache Foundation (Tomcat, ANT, libraries such as Commons, Jakarta, etc.). It is incompatible with the GPLv2, according to the FSF (due to the explicit patent licence) and it is considered that the ASL 2.0 is now compatible with the GPLv3. The importance of this licence lies in the express objective of the FSF to create a GPLv3 licence compatible therewith.

4.1.3.   Other permissive licences

There are a number of permissive software licences that can be seen at the opensource.org website, and commented on the fsf.org website as to compatibility with the GPL. These include, among many others:

- Zope Public License.
- Open LDAP License.
- Artistic License 2.0: a licence modelled on the GPL but without a copyleft.
- Perl: a mixture of the GPL and the former Artistic licence.
- Academic Free License 3.0: A "complete" permissive licence on the MPL model.
- Python 2.0.1, 2.1.1 and later versions: A BSD-style licence, requiring that the program should be subject to the laws of the state of Virginia.
- PHP 3.0: A BSD-style licence including the obligation to incorporate a PHP advertising clause.

- Q Public License (QPL)1.0: A licence compelling the distribution of any modification as a patch to the initial program. It is also necessary to refer to the initial supplier (Trolltech) any modification not available to the public.

4.2. Licences with strong copyleft

Above, we have explained the concept of copyleft from a legal perspective: the obligation to use the same licence for the redistributions of software, with or without modifications, or of a program containing the original software. In this section, we will explain in detail two licences with strong copyleft: the GPL v2 and v3.

We shall see that almost all licences with copyleft are incompatible among each other, as they all require the use of the same licence for redistribution, which gives rise to a conflict in respect of which is to be applied for a program mixing two components under different copyleft licences.

4.2.1. The GNU General Public License, version 2.0 (GPLv2)

Created in 1989, the GPLv2 has been described as being "part licence, part political manifesto": its preamble contains a description of the free software principles and a simple summary of the licence; the main part specifies the rights granted to the users and the limitations and conditions imposed on the exploitation of the software.

> It is important to stress that in spite of its familial and simple tone, the GPLv2 was designed by Richard Stallman with his American legal counsel and therefore does not contain any old provisions, but a deliberate and very subtle means for licensing and conditioning the exercise of copyright rights.

Following we have presented the GPLv2, due to its importance, in some detail.

Useful definitions. Although not explicit, as in the MPL or the CPL, and now in the GPLv3, the GPLv2 contains several definitions that are of great use (and sometimes confusing):

- *Program*: any program or work to which the licence has been attached. Technically, this could include a text, image or other file (clause 0).
- *Work based on the program*: the original program or any derived work thereof, according to the copyright definition. This would include any work containing the program or a part thereof, whether a true or literal copy, or with modifications (clauses 0 and 2).
- *Source code*: the preferred form of the work to subject it to modifications. Regarding an executable file, the obligation to provide the source code includes all modules contained thereby, plus the configuration of the interface and scripts to control compilation and installation. Does not include the source code of the equivalent modules of the operating system

in the program being run, unless such modules accompany the executable (clause 3).

Rights granted by the licence. These guarantee the four main freedoms:

- The right of reproduction and distribution of the original source code (clause 1).
- The right of modification of the program or a part thereof (clause 2).
- The right of distribution of the source code and the future modifications, provided they are distributed with the same GPL and without charging (clause 2b –the copyleft clause–).
- The right of reproduction and redistribution of the program (and its modifications) in object code or executable format, with the same copyleft condition and provided it is accompanied by the source code or the source code is made available to a third party, without charging anything other than the cost of delivery of such source code (clause 3).

   Access to the source code is the second fundamental aspect of the licence. A program may be distributed with the GPL in binary (object code) format, but it must always be accompanied with the source code or the offer to provide it to any third parties for a term of three years (clause 3).

Obligations: the GPL contains several conditions and limitations:

- Any distribution of the program or of work derived therefrom must be accompanied by the notices of authorship, an indication of any modification made (and its date), the disclaimer of warranties and a copy of the licence (clauses 1 and 2).
- It is not allowed to copy, modify or distribute the program in a manner other than that expressly permitted by the licence, with less freedoms or greater restrictions (clause 2b and clause 6).
- If any act in violation of the licence is attempted, the licensee shall waive their original rights (clause 4).

Versions. The licence allows authors-licensors to refer to new versions thereof (we shall discuss version 3.0 below) adding that the work is published "under version 2 and any subsequent version" (clause 9). This flexibility allows that programs maintain compatibility with future programs under a subsequent version of the GPL –such as the recently published GPLv3. In this case, licensees may choose the applicable version.

Other points:

- Warranties. Clauses 11 and 12 clarify that no warranty is offered in terms of the proper operation of the software covered by the licence and repudiate any liability for damages. We have nonetheless seen that the validity of these clauses is dubious (in jurisdictions other than that of the United States and even in the United States in some circumstances) in the light

---

Supplementary content

Linus Torvalds, for instance, has excluded subsequent versions for the Linux kernel: he is staying with version 2.0.

of the consumer protection laws and the prohibition of abusive clauses in accession agreements.

• Governing law. The GPLv2 does not include any clause indicating the governing law or the courts of competent jurisdiction to try any conflicts in reference thereto. Therefore, the relevant law would be applied at the corresponding courts under the principles of conflicts of law. In most cases, it will be the law of the legal domicile of the licensor, but a consumer, for instance, may choose the law and courts of their domicile.

• Patents. The last paragraph of the preamble stresses the dangers that patents pose for free software. The GPLv2, nevertheless, does not include any clause restricting the possible patents on software under the GPLv2 or requiring their licensing in favour of other users (the GPLv3 does). As a logical consequence of the obligation to distribute the program and any work derived therefrom in terms equal to those of the GPLv2 (clause 2b), any licensee obtaining a patent on software under the GPL must allow its free use under the GPLv2 by all subsequent recipients – which could be considered an implicit patent licence. We shall later see that the GPLv3 specifies the terms of the patent licence.

Comments on the GPLv2

An important matter which must be clarified is the matter of **derivative works** and the application of the GPL to them. It is a key concept in understanding the GPLv2, as it defines the scope of the copyleft clause, which is what most distinguishes this licence from other free licences. This matter has given rise to a great deal of controversy in the world of free software and software in general.

> We have already said on several occasions that software cannot be "privatised" under the GPLv2, nor may its derived works. Therefore, some developers doubt to incorporate or relate their work too closely to a copyleft program, as they fear losing them under the GPLv2 in circumstances in which they cannot or do not wish to permit it (such as a non-free development or different free licence).

What does a derived work or work based on a program consist of, according to the authors of the licence? The definition cited earlier refers to the definition under copyright law: it is work containing the program or a portion thereof. But the word contain in the field of programming, leaves room for doubt: are we dealing solely with derived works under a strict legal interpretation of copyright or author's rights? Or does it also apply to "composite works" or collective works, incorporating the original program?

Software components may interrelate in many ways, by various sorts of calls or links. The compiling of a program (to create an executable) may incorporate several components in a single program, or the various components may interrelate when the program is interpreted when run. Each such interaction could have different legal effects. What is debated is whether these architectures imply that the resulting work would be subject in whole or in part to the GPL. This issue has become more complicated with the evolution of program-

ming methods (structured or by objects) and computer languages (C, C++, Visual Basic, Java, PHP, etc.), many of which did not exist upon drafting the licence.

Suggested reading

Slashdot: D. Ravicher on open source legal issues. http://slashdot.org/interviews/01/06/05/122240.shtml

M. Assay. A funny thing happened... www.linuxfordevices.com/files/misc/asay-paper.pdf

L. Rosen. The unreasonable fear of infection. www.rosenlaw.com/html/GPL.PDF

Clause 2b itself states that copyleft applies to any work *containing or derived from the original program*, which must be licensed as "a whole" (with all of its components) under the GPLv2.

- We should first note that the sole gathering or putting together of a work (separable, not based on un a GPL-covered program) on the same medium with GPLv2 software, for distribution for instance, does not imply that such other work must be distributed under the GPLv2. The licence further clarifies that if the identifiable parts of a work could be considered to be individual independent works in themselves, the licence shall not apply to such parts.

- Facing other cases, prudence tells us that it is necessary to assess the risks relating to a particular development or architecture, considering the design and potential consequences of being subject to the GPL. We can say the following with some certainty:
  - If, when a new development is compiled with a GPLv2 work, the final executable includes elements of the original program (in the case of components with static links between themselves), then the modifications may be considered separable and, consequently, the entire work and each of its parts must be distributed under the GPL.
  - If the original GPLv2 program and the new development coexist separately (even when contained on the same medium) and the particular development calls the GPLv2 program in run time (the case of a dynamic link), unfortunately, the situation is not so clear. The interpretation of the FSF is certainly that dynamically linked works, and other forms of interaction such as plug-ins, would lead to relicensing under the GPL if the degree of interaction is sufficiently "intimate" or dependent.

Among the "frequently asked questions" of the GPL, there a few explaining cases of modifications, links and calls to GPL code that the FSF "resolves" by offering its interpretation of the licence and the law. For instance, it is clarified that a new program compiled by a compiler under GPL shall not need to be distributed under such a licence, except if the executable resulting after the compilation incorporates elements of the free compiler or other GPL program.

But the subject is not completely resolved for the GPL and, in the end it is left to the judgment of the creators of modifications and derived works to consider whether they are subject to the GPL (and when to consult with legal counsel).

> Linus Torvalds has expressly included in the GPL covering the Linux kernel of the SO GNU/Linux, an addendum to state that he, as licensing author, does not consider that programs with dynamic links to the kernel are subject to copyleft. User applications and other non-core elements of an operating system, such as drivers, interact dynamically with the components and the modules of the system kernel. Therefore, the applications and controllers are specific to one platform or the other. There is a possibility that such interaction with a GPL operating system could affect such programs and drivers. Without this clarification, almost any program run on GNU/Linux and with calls to its central libraries could be considered, based on the strictest interpretation of the licence, to be subject to the GPL. This would reduce the use and dissemination of GNU/Linux as an operating system to an environment of programs compatible with the GPL.
>
> Nonetheless, over time, L. Torvalds seems to have evolved towards an interpretation closer to that of R. Stallman...

Translations. There are no official translations of the GPLv2. In other words, the original English version shall be that determined by the terms of distribution when the original GPL is applied to a work. There are unofficial translations indicated on the pages of the FSF, which it does not approve as legally valid. It should be noted that if an author applies a translated GPL to its program, the translation of the licence should prevail, not the original GPL in English (except as otherwise indicated). Should there be a translation error, the results could not only be unpleasant, but also horrific for the free software community. There would be "quasi-GPL" versions and modifications of software (with foreign hues) mixed together with true GPL programs (in their English version).

Compatibility of other licences with the GPLv2. A program is compatible from a legal perspective with software under the GPLv2, when distributed in terms that are compatible with those of this licence. They cannot be more restrictive (as in the case of any non-free licence), but may be more permissive (as in the case of the modified BSD licence or the LGPL, which we shall study hereafter).

> Compatibility with the GPL has the dual advantage of facilitating the integration of free components in more complex and integrated distributions and platforms, and ensuring that the code may be integrated fearlessly with 75% of the free software programs available over the internet.

Note that GPLv3 is not compatible with the GPLv2 (but it is with software under the GPL2 "and later versions"), making it necessary for the owners of software under the GPLv2 "alone" to relicense it upon the terms of the GPLv3 (or a more permissive licence) if they wish to ensure such compatibility.

Some examples of incompatibility with the GPLv2

- The Clause of the original BSD licence and the Apache 1.0 licence requiring the inclusion of a mention of the original authors in any advertising or promotional material of the program.
- Clauses reserving rights of the Netscape Public License, allowing Netscape to benefit from third-party modifications to the Navigator and incorporate them into new Netscape products.
- The explicit ASL 2.0 patent licence (in the opinion of the FSF).
- The obligation to obtain a "developer's licence" to be able to integrate Qt elements in applications that are not Windows X System, provided by the Qt licence.

4.2.2.   Version 3 of the GPL

The process of modernisation of the GPLv2 began in 2005 and ended on 29 June 2007, when the FSF published the new GPLv3. Such modernisation responds to various needs, among the main of which are the following:

- Licence internationalisation.
- Improved flexibility.
- Response to author's rights management systems (DRM) and their legal protection.
- Management of legal issues relating to software patents.

To these four items, we could add one more: clarifying the scope of copyleft with respect to new technologies and architectures, dynamic links and the concept of source code.

The main differences with respect to the GPLv2 are discussed below.

a) Definitions. First of all, besides a new definition of Program, You (user) and Modify, there is a new definition: "*complete corresponding source code*" (Clause 1) and two new terms: *propagate* and *convey* (Clause 0).

- The scope of the definition of source code is important, due to the obligation to distribute or offer access to the source code (under the GPL) of any executable distributed without them (GPLv2, Clause 3).
    - GPLv2 defines source code as "the preferred form of the work (program) for making modifications to it" and the obligation to provide the source code includes any "script necessary for compiling the program".
    - In GPLv3, the definition of source code is the same, but the relevant obligation refers to the "complete corresponding source code", which is, a priori, much broader: it includes the "code necessary to generate, install, run and modify (the program)"; the scripts for performing these operations and definitions of interface and (explicitly) the source code of shared or dynamically-linked libraries that the program is designed to use.

- The terms propagate and convey are used, according to the purpose of internationalisation of the licence, to cover all acts reserved by copyright

under any legal system, without mentioning such words as distribute or reproduce, which could be legally defined differently in various jurisdictions.

- Propagate is used to designate "any activity requiring authorisation from the owner of the program", except the running of the program and private modifications (i.e., those not destined for third parties).
- Convey is a subgroup of propagate for the purposes of copyleft obligations (which would activate with the "conveyance"): it means to perform an act of propagation resulting in the creation or obtaining of copies by third parties; for instance, the delivery of a copy to a third party, public communication of the software over the internet, sharing it on P2P networks, etc.

b) Rights granted. While the GPLv2 indicates no authorisation is required from the owner to run the program (considering that the "use" of a program is not subject to copyright), the GPL3 expressly grants:

- The unrestricted right to run and modify the program for private purposes.
- The unrestricted right to propagate the program, provided it does not result in the conveyance of the software. This would therefore include the right of reproduction, modification and internal "distributions". It also allows the delivery of the software to third parties unconditionally, when done under a consulting agreement whereby the consultant is to make modifications exclusively for the licensee (work-for-hire).
- The right to transfer the software under copyleft conditions.

c) Obligations. The basic obligations with respect to the copy and the distribution of the software are similar to those established in the GPLv2: it is necessary to maintain notices of authorship, the licence, notifications of changes, etc. If the program has a user interface, it must contain a system for publishing copyright notices, the disclaimer and the access to the licence –an obligation stronger than that of the GPLv2.

Regarding the copyleft system, the GPLv3 does not change much either:

- It maintains the obligations to convey any modified work "as a whole" "under the same licence" (letter 2b of the GPLv2, now 5c).
- It slightly modifies the obligation to accompany any distribution of binary code with the "complete corresponding source code" or offer access thereto to any third party who has the binary. The term of this offer is the greater of three years, or the duration of any medium or offer of "corrections". The cost of its distribution may also be charged.
- It specifies five ways to make this distribution/offer (such as, for instance, distribution on CD, from internet servers or sharing on P2P networks).

d) DRM. In Module 2 we discussed the legal system of protection of copyrights management systems (Digital Rights Management or DRM): it is illegal to "circumvent" (i.e., crack) an effective technological measure, capable of protecting author's rights. The GPLv3 has two mechanisms against those systems, which it considers a violation of the freedom of the users (the FSF calls them Digital Restrictions Management):

- On the one hand, its Clause 3 states that by no means shall GPLv3 software be considered part of an "effective technological mechanism of protection" of rights and that the owners waive the right to sue third parties for any act of elusion resulting from the mere exercise of the rights assigned under the licence. By these indirect means, it seeks to allow that any GPLv3 software be modified without infringing upon such rules, which would prohibit that type of "circumvention". The consequence sought is that it will be incompatible to distribute GPL3 software on DRM programs whose licence does not allow access, modification or reengineering. Whether this works legally is a subject of debate, especially considering the imperative nature of the system of protection of these DRM systems.

- On the other hand, the GPLv3 includes, in the definition of "complete corresponding source code", exceptionally for consumer products, the access and deciphering keys and the information for installing and running modified software. With the GPL3, manufacturers and distributors of "closed" devices for users / consumers cannot prevent access to the device or demand obtaining payment for a key, for instance, to "access" or run the device or modify its program code. If they did, they would also have to surrender the keys, codes and the relevant information.

e) Patents. The patent protection system in the GPLv3 is complex, due to the various practices that have arisen in terms of software patents. Under GPLv2, any assignment of patent rights (to a process implemented with GPL software) was implicit, with the consequent uncertainties in terms of its legal effects. In GPLv3, there are four important terms (Clause 11):

- The assignment of patent rights is made explicitly: if someone has a patent on their contribution to software distributed under GPLv3, it grants a patent licence to use, market and import the contributed software to anyone using such contribution without modifications.
- Any explicit patent licence granted to a licensee shall be extended to all licensees.
- Additionally, a "cascading" protection mechanism is sought to be established: those distributing software under GPL3, benefiting from a patent licence from a third party, must extend its benefit to all licensees, or waive the benefit, or guarantee that the "corresponding source code" is available to all under the conditions of GPLv3.
- Regarding the agreement between Microsoft and Novell of March 2007 (not to be covered by the licence), if someone obtains specific protection

in respect of software under the GPLv3 that, in a discriminatory man-
ner, may solely protect them and their licensees, such software cannot be
transferred under GPLv3.

f) Remote services or Application Service Providers (ASP). It was thought
that the new licence would restrict the use of GPL software by those offering
commercial services to their end users based on GPL software, without dis-
tributing their programs and sources (Google and Yahoo! are obvious exam-
ples) or that they would be compelled to furnish the source code of any ASP
service. In the end, this mechanism has been left for the Affero GPL and an
explicit compatibility is included with the licence.

g) Additional permissions. The GPLv3 allows adding some additional per-
missions (but not restrictions), such as exceptions from its obligations. These
shall apply to identified software components and may be eliminated by the
licensees upon redistribution. The LGPLv3 is an example of this, as it consists
of the GPLv3 with the additional permission to link to programs "using the
library" under any licence (as we shall see hereafter).

h) Additional restrictions: licence compatibility. The "legal compatibility"
of the software is fundamental in the development of free software: it means
being able to mix two programs with different free licences, without either
being in breach in redistribution. The GPLv2 prohibits adding any addition-
al restriction not included in the licence itself. This has led to licences with
agreements in respect of patents, attribution of authorship, use of trademarks,
notices and disclaimers with differing terms, being declared "incompatible"
with the GPLv2 by the FSF (and by attorneys advising their clients). The
GPLv3 makes an effort to enhance the set of free licences compatible there-
with through a new mechanism: allowing the addition of six types of addi-
tional restrictions on programs or code added to the GPL3 code.

> The restrictions are compatible if they refer to:
>
> - Maintaining notices of authorship or other forms of attribution (for instance, notices
>   of "powered by" or "about" windows) and obligations to indicate any modification
>   made to them.
> - Disclaimers (warranty exclusions and liability limitations) in terms other than those
>   of the GPL3.
> - How to indicate modifications.
> - Restrictions on the use of the names of authors for advertising purposes (the former
>   BSD licence continues to be incompatible).
> - Granting rights or prohibitions in respect of the trademarks.
> - Indemnities for contributors.

The Apache 2.0 licence is an example of licence that is now GPLv3 compatible.

4.2.3. Other licences with strong(er) copyleft

While the GPL is considered to have (debatably) the strongest degree of copy-left, encompassing both derivative works and works which, on a wider interpretation, could be considered based or dependent on the GPL code (or contain it), other free software licenses have a strong copyleft effect.

Common and Eclipse Public Licenses. The CPL and the EPL (and their predecessor, the IBM Public License) are legal instruments developed by IBM, with a format differing from that of the GPL and the BSD, the two predominant models. The CPL is closer to the Mozilla Public License, as it has a more "legal-like" form (including definitions and governing law) and covers such issues as indemnities among contributors and patent licences. They are well drafted licences from a legal perspective and leave much less room for doubt than the GPLv2, for instance. Definitions are clear, as is the scope of the rights and obligations. Our main comment is that the licence is incompatible with the GPLv2 due to the obligation to license any patent of the contributors and compensate the co-authors in the event of claims by commercial users (cross-indemnity among contributors). A priori, we understand that this continues to be incompatible with the GPLv3, although it too has a quite similar patent licence, as regards commercial indemnification.

Aladdin Free Public License (AFPL) The Aladdin Free Public License (AFPL), relating to Ghostscript, warrants special mention as it has a particular nature. It does not comply with OSD, although it is directly inspired by the GPL. What is interesting is that, while the latest available version of Ghostscript is distributed under the AFPL and requires obtaining a non-free licence for commercial uses, the penultimate version of the software is released under the GPL. Therefore, the "best" version of the program is marketed and free developers may take advantage of the oldest code.

Sleepycat Software Product License (Berkeley Database). This is a licence applied, most of all, to a database engine of the Sleepycat corporation (formerly Berkeley Database). It follows the simple model of the BSD licence, which we shall discuss hereafter, and adds an obligation to distribute or make available the source code of the software and of any other program using the software. Such a program must also be freely redistributable under reasonable terms (copyleft). Open and free licences are considered reasonable, as is the GPL.

GPL Affero 1.0. Affero is software for managing and extending virtual communities with rating and e-commerce functions. The licence is a variation of the GPLv2, drafted with the aid of the FSF. The licence covers the case of the architecture of programs distributed on networks or services linked by web services. In this case, the user / licensee does not receive the program as software distribution, but as a web service, and may offer the same service to third parties, avoiding the copyleft obligations of Clause 2b. The Affero licence adds to the GPLv2 a Clause "2d", which provides that if a service offered over the

web by the original program were to have a function to provide the source code also over the web, the licensee cannot eliminate that function and must offer access to the source code of the derived work over the web.

Affero GPLv3. The new Affero GPLv3 licence is basically the GPL with an additional agreement to cover the same scenario as mentioned with respect to Affero 1.0. In this case (ASP), users of remote services must be granted access to the source code. The GPLv3 is expressly compatible with Affero GPLv3 and vice versa.

Licence OpenSSL / SSLeay. This licence applies to SSL security programs. It is a combination of the Open SSL and SSLeay licences. It is modelled on the BSD licence and adds to the end of the SSLeay licence a copyleft clause requiring that any derived work be distributed upon the same terms. Mixing this code with GPL code is expressly prohibited. It is also incompatible with the GPL inasmuch as it has a clause with respect to advertising and the attribution of authorship (derived from the earlier version of the BSD and the Apache).

4.3. Licences with weak copyleft

In this section we shall discuss free licences that are known a having a weak copyleft effect: they are distinguished from strong copyleft in that they allow for their integration, use and redistribution in programs subject to other licences, but maintain their own code subject to copyleft.

4.3.1. The GNU Lesser (or Library) General Public License (LGPL)

The GNU Lesser General Public License (or Library GPL) is the second licence drafted by the Free Software Foundation. Initially, this licence was known as the "Library GPL", as it was designed expressly to be applied to computer libraries.

> The FSF later changed its name to "Lesser GPL" as it considered that it guaranteed less freedom than its older sister, the GPL. Its version 2.1 is of February 1999 and, in June 2007, version 3.0 was published, which is a variation of the GPLv3, discussed above.

In the preceding sections we have mentioned that when a program links to a software component, whether it be statically or through a dynamically-shared component or API, the combination is considered a work "based on" or "derived from" the original software. If the software is under the GPL, many argue that this link would force distribution of the entire final program under the GPL. The LGPLv2 was created specifically to allow certain free software components –libraries – with non-free programs, without affecting the resulting program. Therefore, a library with LGPLv2 offers a certain comfort or certainty for the developers of non-free applications wishing to link their programs with components under free licences, but that fear the copyleft effect of the GPL.

Supplementary content

The LGPLv2 derives from the GPLv2 and most of its terms are similar to those thereof. We therefore refer to the section on the GPL (both version 2 and version 3). Here we shall solely comment on its distinguishing elements.

As for the GPL, the LGPLv2 defines program and source code. It also includes three new definitions:

- **Library**: consists of a series of software components destined for linking with programs (using the functions incorporated in libraries) to create an executable.
- **Library-based work**: contains the definition of program in the GPL and means the original library or any derived work thereof, according to the definition provided by copyright law, i.e., work containing it or part of it.
- **Work using a library**: is separate work containing no part or derived work of the library, but rather is destined for being run with the library through compilation or links.

Regarding the same library and its modifications, the conditions applicable are those of the GPL. The main difference with the GPL is that the LGPL allows for the unrestricted distribution of an executable, consisting of the compilation, on the one hand, of works using the library and, on the other, the library itself (Clause 6). This is the exception to the regular copyleft clause of the GPL.

> Nonetheless, the recipient must be allowed to modify the program (even the work "using the library") for particular use and for performing reverse engineering operations to correct errors (therefore, it is argued that although there is no copyleft, it remains necessary to provide the source code).

As an additional condition, the LGPL applied to its library may be converted into the GPL at any time (there is no turning back) (Clause 3). We should also note that the LGPLv2 is compatible with the GPLv2, but not with GPLv3 or LGPLv3.

Due to its language, the LGPL is destined for use by libraries. But its use is not restricted to them, as there are other programs distributed with this licence (for instance, OpenOffice.org). The authors of the software are free to use the licence of their choice, regardless of their program.

> The FSF no longer recommends the use of the LGPL, except for strategic reasons: the use of the LGPL allows the broader distribution and use of its code and, therefore, favours the establishment of a component –a library, a program module etc.– as the standard in the sector. The LGPL does not, however, favour the development of free applications, which is a fundamental objective for the FSF, and therefore does not receive its full approval.

As a practical comment, we should note that, within the limits of the technical matters of the type of link between two programs, it is possible to combine, integrate and distribute libraries under the LGPL with software under any other licence, even non-free. An example of this type of software is the C library (libgcc) distributed with Linux, which may be used to develop non-free programs running on Linux.

LGPLv3

LGPLv3 is an explicit variation on GPLv3, i.e., it is GPLv3 plus additional permissions. Such permissions authorise the use of the library in question by a third-party program and licensing "as a whole" under a licence other than the LGPL. It also does not apply Clause 3 on DRM systems.

4.3.2. Mozilla Public License

The Mozilla Public License (MPL) was developed along with the Netscape Public License in 1998, when Netscape "opened" (as open software) the code of its internet browser, Netscape Navigator. The development of the licence was a collaborative effort between several of the "gurus" of the open movement, such as Linus Torvalds, Bruce Perens and Eric Raymond. They initially sought to persuade Netscape to use the GPLv2, but facing the refusal by Netscape and the need to respect the intellectual property of third parties, they ended up distributing the code under the NPL.

> Consulting with the community. Before opening its source code to the public, Netscape distributed a draft of the proposed licence on a newsgroup created especially to gather opinions on the matter (netscape.public.mozilla.license). The process of open development for the software carried over to the free world and awoke great enthusiasm... and criticism. There were several proposals to modify some of the terms of the NPL, especially that which allowed Netscape to use the same code in other products not under the NPL. This process has been followed by the Free Software Foundation in drafting the GPLv3.
>
> In the end, seeking balance between the commercial and free development objectives of Netscape and the free community, it was resolved to issue two licences: the NPL and the MPL. The first was applied to the initial code of the Navigator and to the modifications made thereto, and is no longer used. The second was applied to any software added to the code and to any completely- new program wishing to use the licence. The MPL is now used for several programs, including the Firefox navigator and other programs from Mozilla.org. The two licences are identical, except for some rights reserved by Netscape in the NPL for its initial code, which is only of "historical" value.

The MPL has a classic software licence structure and begins with important definitions permitting, among other things, distinguishing between what is original code and what is added code.

- **Initial developer**: in the case of the NPL, Netscape; in code under the MPL, the initial author indicated in the annex to the licence and any author of contributions.
- **Initial code**: code distributed by initial developers.
- **Modification**: any modification to the covered code not including a simple addition of a new separate file or a new code acting with the original code without modifying it (for instance, through an API –even if the API itself could be a modification, if integrated in the covered code. The word "modification" does not refer to the entire new work (as is the case with the GPL), which may also be a "derived work" under the law, but rather refers solely to the modified part.
- **Covered code** (covered by the licence): initial code plus modifications.
- **Contributor**: any third party modifying the covered code.
- **Larger work**: a work separate from the covered code but that may incorporate it or may link to it, without modifying it (Clause 3.7).

The meaning of "modification", summarised here, clarifies many things that the GPLv2 did not make clear –especially the matter of additional new files that do not modify any part of the initial code at development. It therefore allows a developer to add separate files and programs (non-free or free) and distribute them separately from the covered code, but as part of a larger program (potentially non-free).

a) Rights granted. As with all free software licences, the initial developer, first, grants a licence for the free use, reproduction, modification and distribution of the code and, second, a patent licence that is sufficient to allow the use of the program and modifications (Clause 2.1).

- Each contributor provides similar licences in relation to their contribution or modification (Clause 2.2).
- The code may be distributed in binary under a licence compatible with the MPL, provided the obligations contained in the licence are respected, such as access to the source code, for instance (Clause 3.6).
- The covered code may be included in a "greater work" (including it, but not modifying it) under any licence, provided the obligations relating to the covered code are respected (Clause 3.7), for example, access to source code.

b) Obligations. The source code of the initial code and any modification (covered code) must be distributed under the MPL, without more restrictive clauses (copyleft for the covered code, Clause 3.1). If the covered code is distributed in binary, access to its source code must be offered to the recipient of the distribution for at least twelve months (Clause 3.2). It is necessary to accompany any modification with a copy of a licence and an indication of the modifications and their authors, and indication of any known claim to the code (legal.txt) (Clause 3.3-3.5).

The MPL is a complete licence –imitated to some extent by the CDDL, the CPL, the OSL and now, dare we say it, the GPLv3. It is a much more clear and complete licence than the GPLv2 and, evidently, than the BSD. It was drafted with and by attorneys in the context of a commercial company and thus includes specific definitions and contains traditional matters relating to licences, such as competent jurisdiction and governing law.

Although its effect could seem closer to the BSD than the GPL, there are several important matters that we must consider and we shall discuss in this section:

- The MPL has partial reciprocity or copyleft, as does the LGPL: the covered code (including any modification) must be kept under the MPL, while any extension (larger work) may be non-free. It is also very easy to create an additional non-free file calling the original code under the MPL and distributing it entirely under a non-free licence. This continues with the philosophy of the BSD licence. Nonetheless, in all cases, the source code of the original free part must be distributed or offered to the recipient. This may all be illustrated as follows:

- Any software under the MPL 1.0 (and the MPL 1.1 with no alternative licence) is incompatible with the GPLv2 and the GPLv3; fundamentally as it contains too many additional restrictions relating to patents (although the GPLv3 is close in that aspect) and the possibility of linking to non-free programs, among other things. The possibility of multiple licences offered by version 1.1 allows compatibility if the GPL is chosen as an alternative licence (the source code of the programs of Mozilla.org, for instance). Figure 3. Illustration of persistence of the MPL.

- Patent clauses. As we have already seen in relation to the GPLv3 and the CPL, the termination clause (in this case clause 8), combined with the patent licences (Clause 2.1), is part of a new generation of clauses in free licences to create a work environment free of patents and free of the risk of patents. It constitutes what is known as "patent cross licensing". Developers cannot prevent a person from requesting and obtaining a patent on a process that may be part of a modification of the initial program (in the United States). The risk is that the use or a subsequent modification of the software could infringe upon a patent if the user does not use an appropriate patent licence.
  These clauses therefore seek two things:
  – *On the one hand, the "patenting" person must grant all other licensees (users and developers) a patent licence with respect to the patented process or code included in their contribution.*
  – *Additionally, the licences of author's rights (and patents, if any) granted to such "patenting" person shall be cancelled in the event of any litigation or attempt to prevent the free exploitation of the modification.*

- Commercial balance. The concepts of modification and larger work have been carefully prepared to find a balance between the freedom of the BSD, allowing an unlimited use of the code and the freedom of the GPL, requiring that all code and free derived works should be maintained, i.e., between the promotion of the development of free software by commercial companies and the protection of the work of "free" developers. This fair mid-ground has been defined by the difference between a modification and an addition. We should bear in mind that the GPL, in contrast, affects the additions intimately linked to software under the GPL.

- *legal.txt*. This is a file where the contributors must include notices of any claims, litigation or restriction on any part of the code. It evidences a clear knowledge of the process of free development, in which the risk of claims relating to intellectual and industrial property is high and transparent information is essential. A subsequent developer must use this file to study the legal limitations of code provided by third parties, perhaps in relation to a patent litigation, perhaps due to the limitations of certain parts of the code that may be under a licence that is compatible but differs from the MPL...

4.3.3. Open Source License (OSL)

The Open Source License (OSL, now version 3.0) is a licence with a weak copy-left, drafted in a neutral manner by the legal advisor of the OSI, Lawrence Rosen. It is a complete licence (definitions, licence explicit to the various rights, etc.) and conforms better than others to the legal framework of intellectual property in Europe and limitations regarding warranties and liabilities.

The OSL 3.0 limits its copyleft effect to *derived works according to the intellectual property law* applied in each case. It is argued that the GPLv2 is sought to be extended beyond what is permitted by author's rights alone (reproduction, modification, public communication and distribution) and could be limited by a strict interpretation of the law. The scope of the copyleft of the OSL is strictly within the scope of exclusive rights of the authors under intellectual property.

> This would allow, for instance, the linking software under the OSL 3.0, as libraries or with dynamic links, and the licence would not "affect" the software using such libraries, to the extent that they were not "derived works" of the original software.

Beyond the copyleft provisions, the definition of governing law and competent jurisdiction (in favour of the licensor) is more favourable for the authors and software distributors. Additionally, with an express warranty of title to the software and coverage in respect of wilful misconduct and personal damages, the warranty and liability limitations shall be more valid in Europe. Finally, distribution within a group of companies is not considered distribution for the purposes of copyleft obligations, as is the distribution of the services provided by the software (in ASP or "SaaS" mode) in which case it would be necessary to provide the recipient of the services a copy of the source code.

4.3.4. Other licences with "weak" copyleft or "hybrid"

There are a number of other free software licences following the weak copyleft model or tenets of the LGPL and the MPL. Each licence has been created for a specific or generic purpose, and must be understood and chosen in accordance with its own wording and merits applied to the specific case.

Apple Public Source License v. 2: A variation of the MPL created by Apple, with new elements, such as governing law (California), and covering the possibility of offering services over the internet (externally deployable), similar to the Affero.

CDDL: This is a generic version of the MPL created by Sun Microsystems with some modifications and without the commercial name Mozilla. Used for OpenSolaris, among other programs. The main differences with the MPL is that it does not include "scripts for the creation of executables" or API, etc., in the definition of source code. In case of distribution of the binary, the source

code must be generally published (not limited to distribution recipients). The *legal.txt* file of the MPL has been eliminated. The patent peace is limited: the patent licence is revoked in case of claims based on patents with respect to processes implemented by the covered code. Governing law is flexible, defined by the original owners. Copyleft includes distributions of services of the program to clients in ASP mode (sources must be offered to the service recipient).

EUPL 1.1. The European Union Public Licence is a new licence (of January 2007), expressly drafted for the release of software by the European Public Administration and the member countries of the European Union. The scope of copyleft is similar to that of the OSL, it contains a patent licence and the limitations on warranties and liabilities are valid within the general consumer protection framework and the accession agreements of the European Union. To establish an express compatibility with other copyleft licences, it contains a compatibility agreement with other licences included in an attachment (currently the GPLv2, the LGPLv2, the OSL, the CPL and the CeCiLL, a French copyleft licence): in case of mixing software under the EUPL with software under such licences, the software could be distributed under the new licence. The European Commission has published official translations in the languages of the European Union.

eCos licence 2.0 and Classpath. This is an FSF licence on the Embedded Configurable Operating System. It basically consists of the GPL plus an exception that allows linking the program to other programs that are not under the GPL and with effects quite similar to the LGPL. Whether integrated by compiling or linking to a non-free program distributed in binary, the eCos source code must be provided or made available. Classpath contains the same exception. What is interesting to note is that Sun has published a large part of the Java platform under the GPL, with the exception of Classpath.

CPAL: Common Public Attribution License is a variation of the MPL, with an explicit "Attribution clause" that requires publishing either on the user interface or another manner, attribution to the original developer of the code.

4.4. Other "free" licences

In the previous section we studied in depth the main free licences and discussed their features, their compatibility and consequences. In this section, we wish to complete our analysis of "free" licences. We will comment, in order, the following:

- Licences that we shall refer to as "pseudo-free", seeking to emulate free licences but containing a restriction that does not meet the freedoms of the FSF or OSD guidelines.
- Free documentation licences.
- Freeware and shareware licences, which are by no means "free".

4.4.1.   The rise and fall of "pseudo-free" software licences

Although in this module we have focused on free software licences, it is interesting to present a brief analysis of the licences created by commercial enterprises seeking to benefit from a free development model –without paying all its "costs". First of all, this is indicative of the array of possibilities between free and non-free. It also allows clarifying the position of such companies in that regard and indicating some strategies that must be avoided from the viewpoint of free licences. We have observed that the role of Shared Source licences has diminished, due to the trust and popularity gained by truly-free software licences, and the criticism received thereby at the time.

The Sun Community Source License (SCSL) was an attempt to offer access to the code and programming environments of Sun Microsystems Inc., for instance Java or Jini, and to establish it as a standard. In this sense, it has had great success, especially in terms of Java. The "components" included in the Sun Community License were J2EE, the Java Developers Kit (JDK), Personal Java and Embedded Java, among others. The shared source era of Sun has nonetheless almost ended, inasmuch as in November 2006, Sun Microsystems released most of the programs forming the Java technological environment under the GPL (with the exception of Classpath).

The SCSL was, above all, a licence for developers. It is "open" mainly for research and development purposes, but allows Sun to maintain a strong control of the evolution of the program and programming environments. Conceptually, it was a licence that was halfway between the MPL and a non-free licence: it allows corrections, modifications and extensions, but any of these must be returned to Sun.

In 2006-2007, pressured by the free community, the rise of new free projects to create Java technologies to replace Sun software and the acceptance by Sun of the benefits of free software, the company began to adopt a position more favouring free software. It first opened Opensolaris, its operating system, under the CDDL and created a project and a community around the software. It later published its part of the patent pledge against Opensolaris users. Finally, in November 2006, it released its Java technologies under a GPLv2, with the Classpath exception (which allows using the libraries without a copyleft effect).

4.4.2.   Microsoft Shared Source Initiative (MSSI)

Microsoft also created a series of over ten "semi-free" licences for part of its programs. They applied to the CE operating system for portable devices, CLI (Common Language Infrastructure) and the specifications of C#, and also included elements of Windows 2000 and XP. This "gesture" especially allowed the academic study of the technologies in question and, for commercial companies creating products running on such platforms, a better integration of

MSSI

About the MSSI, see the Microsoft website.

their programs with those of Microsoft. It also allowed Microsoft to disclose the source code of several applications to government organisations, under very strict secrecy conditions.

There were several types of licence as part of its Shared Source initiative. The basic model, for instance, the Shared Source licence of CE, opened the code to researchers and students: the source code could be downloaded and studied, and code modifications could only be used, modified and distributed for non commercial use, provided the same licence was maintained. Later, with the Windows CE Shared Source Premium Licensing Program, manufacturers of OEM devices had access to the source code of Windows CE and the right to modify and distribute the modifications commercially. They were nonetheless required to license any modification to Microsoft free of charge, allowing for it to incorporate such modifications in subsequent versions of the software after a six-month period.

> Other MSSI licences contain variations of these rights granted and reserved. The licence for ASP.net, for instance, allows any commercial and non commercial use, but prohibits combining and distributing the ASP.net program with any free programs and especially under copyleft conditions.

In October 2005, Microsoft reduced its Shared Source licences to five: three basic licences and two variants, limited to the Windows platforms. The three basic licences are:

- **Microsoft Public License (Ms-PL)**. This is a permissive licence, copyleft for distributions made in source code format, but permissive for distributions in binary format. Contains a variation limited to technologies for Windows. Approved by the OSI and compatible with the GPLv3.

- **Microsoft Reciprocal License (Ms-CL)**. This is a reciprocal licence or copyleft, with effects similar to that of the Mozilla licence: the copyleft effect is defined based on the original files and the files of a "greater work" (using the original files) may be distributed under any licence. It also has a variant limited to technologies for Windows. It is approved by the OSI but not compatible with the GPL.

- **Microsoft Reference License (Ms-RL)**. This is a licence similar to the former Shared Source licences, which allows copying the program for internal use, but not its modification or distribution.

4.5. Free documentation licences

Free licences are applied mostly, but not exclusively, to software. A series of free licences have been created for documentation, especially as software is accompanied by technical documentation, which is often necessary for its use. It would not make sense to distribute free software without distributing the relevant documentation under similar terms. This led the FSF to create

the General Free Document License to accompany its programs. Additionally, following the trend to open knowledge, other licences have been created on documentation and materials, especially academic. We shall present an example: the Creative Commons initiative.

4.5.1. The GNU Free Documentation License (GFDL)

The GFDL is generally used for licensing technical documentation, user manuals and other relevant texts for free software. It is modelled upon the GPL, but changes its conditions to adapt to written text rather than software. The licence seeks balance to allow modifications (especially those necessary to document a modification of the software), maintain the authorship of the initial work and respect the ideas and opinions of the original authors.

The licence defines several elements of a document to establish the rights and obligations corresponding to each, for instance "secondary sections" (legal notices, dedications, acknowledgements, etc.) and "invariable sections" (secondary sections that cannot be modified).

The GFDL grants several rights relating to copying, distribution, modification, aggregation and combination, collection and translation of the original document. These rights generally granted, subject to the respecting the original authorship, maintaining certain identified parts of the text unchanged, and supplying access to a "transparent" version of the document (the equivalent of the source code of a program, being a legible copy, modifiable by a third party using free or generic programs, such as ASCII, XML with public DTD, HTML formats, etc.,).

Transformation of the text gives rise to a series of obligations: any derived work must change the title on the cover, indicate the original authors and any modifications, indicate where the original version may be found and maintain copyright notices and the licence. Additionally, certain defined sections must be maintained and the tone and general content of the secondary sections must remain unaltered. Any indication of endorsements must be eliminated from derived works.

As the GPL, the GFDL maintains the copyleft of the documents: any modification must be distributed under the same licence and cannot be combined with text from work under a more restrictive licence.

The licence not only applies to technical documentation for software. It may also be used for any text, specifically any "literary" work developed as free software: in collaborative works. In fact, Wikipedia (at www.wikipedia.org) is published under the GFDL.

In 2008, a new minor release of the licence was published, version 1.3, so as to achieve compatibility with the Creative Commons BY-SA 3.0 licence which we comment below. This is mainly so that wikis such as Wikipedia can use content under this CC licence in the wiki.

The GFDL is not the only free documentation licence. In part due to the controversy in relation thereto, many free software projects have created their own licences: the FreeBSD Documentation License, the Apple Common Documentation License or the Open Publication License, and the OR Magazine License (by O'Reilly).

4.5.2. The Creative Commons initiative

The Creative Commons initiative, often abbreviated to CC, is a project of Stanford University, in California, created by a series of copyrights experts, including Prof. Lawrence Lessig. It seeks to aid authors and creators to freely distribute their works for use by the public, thus increasing the number of creative works available to all. It is especially directed to literary and artistic creations and not software, and expressly recommends the GFDL for any computer documentation. Additionally, the CC proposes a private system, under United States law, to limit the duration of copyright protection to fourteen years, rather than the term agreed by law (generally, the life of the author plus seventy years) based on a public statement. Finally, it allows dedicating works to the public domain, also under conditions of United States copyright.

Some rights reserved. The Creative Commons[9] initiative operates under a slogan that is a play on words on the regular copyright reserve of "all rights reserved". The slogan is "Some rights reserved", similar to that of the FSF, which is "All rights reversed". The freest CC licence would even allow including the expression "No rights reserved".

[9]The Creative Commons project may be found at creativecommons.org.

In addition to a generic version of the licence, which is sought to conform to the international conventions on author's rights, there are versions adapted to the legal framework of each country: Spain, Peru, England, Japan, etc. (and linguistic versions, in Catalan, for instance). The latest generic version, 3.0, contains a compatibility agreement to allow the equivalence of licences between these "local" versions.

The strategy of the CC has been to create a series of modular licences establishing what rights are granted to the licensees.

The licences contain a core of terms that are common to all variants and then particularities regarding the grant of rights. The core elements include:

• Notices of authorship and copyright are required to be maintained ("BY").
• Internet links may be established in works published on such medium.
• No modifications to the licence are permitted.

- No technological mediums may be used to restrict the legitimate use of the work (in other words, no DRM technologies).
- They apply in all countries of the world.
- They are irrevocable and have a duration equal to the term of the copyright protection.
- They offer a warranty of ownership and non violation of third-party rights (to increase confidence in the reuse and redistribution of the work).
- The author or owner of rights is allowed to distribute the work under a different licence.
- They contain a special exception allowing P2P file-sharing, which is not considered a commercial activity, provided it is not for profit.

Regarding the grant of rights, authors may choose the rights that are reserved and granted in the licence based on three criteria:

- Commercial use ("NC", for non commercial use restriction).
- Allowing derivative works or not ("ND" – no derivatives).
- Reciprocity or copyleft ("SA", for share alike).

The website www.creativecommons.org also contains an automated tool for creating the licence based on the answers to questions on such criteria. A CC licence is proposed to users upon the basis of two questions:

- Whether or not to permit commercial use:
  – Commercial. Allows any type of use, including commercial.
  – Non commercial (NC). Allows any type of exploitation and derivation, provided it is for non commercial purposes.

- Whether or not to allow the creation of derived works:
  – No derived works (ND). Modifications are not allowed for the creation of derived works.
  – Share alike (SA). If derivative works are allowed, then redistribution of the work and derived works must be solely upon equal terms as the original licence (copyleft).

Thus the most basic and permissive licence is the Attribution license (BY), which merely requires that credit be given where due and allows everything else, similar to a BSD style free software licence: no commercial restriction, no share alike.

The Attribution-NonCommercial-ShareAlike (BY-NC-SA) allows modification, requires maintaining the same licence in derived works and prohibits commercial use. The MIT OpenCourseWare licence is of this type. Another text with this licence is "HOWTO: Installing Web Services with [free software]".

The Attribution-NonCommercial licence requires that credit be given where due and restricts commercial uses. The Electronic Freedom Foundation, at www.eff.org, uses this licence.

The tool creates and offers the user the text of the licence. Licences come in three formats:

- An easy to read version: a very easily understandable summary ("Commons deed" or "Human code"), with icons, which we shall mention hereunder.
- A legal version for lawyers: the complete version of the licence ("Legal code").
- A machine-readable version: an expression in RDF and XML metadata so that an automated computer process may understand the licence in the context of the semantic web ("Digital code").

4.5.3. Freeware and shareware licences

We only wish to stress here that shareware and freeware licences are not free software licences. Although the relevant programs may be distributed free of charge, they do not provide access to the source code and, in their majority, they do not respect the minimum conditions for being free or open: the four basics freedoms of the FSF or the OSD definition.

5. Free software licences in practice

After the previous analysis of free software licences, this section starts with a comment on and clarification of certain myths or misconceptions with respect to various legal aspects of free software. We then comment on several key issues related to free software licensing, including how to choose a free licence, the issues raised by contributions to free software projects, compatibility between licences, and other topics.

5.1. Some legal myths about free software ... to debunk

Over the years certain myths or misconceptions have arisen with respect to various legal aspects of free software, not least due to FUD (Fear Uncertainty and Doubt) spread by those who do not necessarily agree with the tenets of the free software movement. Here, we comment on these misconceptions and try to determine the truth of fallacy behind them.

> There are other myths relating to the technological or commercial aspects of free software that we shall not address here: lack of support and maintenance, lack of security, risk of forking, the possibility of introducing damaging elements in free software, lack of viable business models based on free software, etc.

5.1.1. Copyleft goes against author's rights

This myth is based on the belief that copyleft (and free licences in general) creates a new intellectual property legal framework: *copyleft* "rather than" *copyright.*

Quite the opposite, as seen above, free software licences are based directly on the current author's rights or copyright law, whether it be author's rights under continental style or the copyright of English-speaking countries. The authors of free software use the rights established by this legal framework (exclusive rights to exploit and/or authorise the exploitation of their work) to grant the licensees the non-exclusive rights established in the free licences and defend these rights from infringement.

> In MySQL AB vs Progress Software, MySQL AB defended its ownership of rights in the database application MySQL. It initiated proceedings against Progress Software for the violation of author's rights and of the licence terms of the GPL to the MySQL program.
>
> In Germany, the several courts have now decided in favour of the rightsholders in the netfilter/iptables project, in relation to infringement of the terms of the GPL based on authors' rights / copyright law. They could thus enforce the licence obligations on a licensee who had breached the terms of the licence and (for distribution without the source code and without a copy of the licence) thus potentially infringed their copyright.

Let's consider, for instance, two important characteristics of free software: freedom of use and copyleft conditions.

- Regarding the first, the legal framework allows the owners of work to de-fine the scope of the exploitation rights granted to third parties. Rather than restricting the uses (as is done by most non-free licences), a free soft-ware licence permits them to the maximum permitted by law. This does not go against author's rights, but rather is an exercise thereof.

- Regarding copyleft, a developer may create and distribute a derivative work of free software as permitted, under certain conditions, by the owner of the original work on which it is based. If such conditions – for instance, to distribute the derivative work under the same licence (copyleft)– are not met, the original licence shall be cancelled and the distribution of the derived work shall constitute a breach of the copyright rights of the licen-sor. The copyleft acts legally as a termination clause.

> In the USA, in Jacobsen v. Katzer the US Court of Appeals held that Artistic licence terms were enforceable conditions on the permission to exercise copyright rights granted in the licence, and therefore a licensee in breach of the licence would be in breach of copyright, the licence being revoked.

Therefore, there is no contradiction or opposition between legislated author's rights and the rights granted or reserved under a free licence. Moreover, it could be argued that, given that a free software licence respects the exceptions and uses permitted to the user under our legal framework, it conforms better to the law than many non-free licences.

> **E. Moglen, "Enforcing the GNU GPL", Linux User, 12/08/2001**
>
> "The GPL, on the other hand, subtracts from copyright rather than adding to it [user restrictions, for instance]... Copyright grants publishers power to forbid users to exercise rights to copy, modify, and distribute that we believe all users should have; the GPL thus relaxes almost all the restrictions of the intellectual property system".
>
> **Enforcing the GNU GPL**
>
> Article to be read online at E. Moglen's site.

5.1.2. Free software has no owners

There is nothing further from the truth, from a legal viewpoint. The author's rights/copyright legal framework automatically grants author's rights to the creators of software. And the sole obligation –or almost sole obligation– com-mon to all free licences is to maintain the notices of the rights of the initial creators of the software (the famous "copyright notice"). There is therefore al-ways an owner of the rights to the software and, in the case of free software, ownership is clearly indicated in the files.

5.1.3. Free licences compel authors to assign their rights

With the exception of moral rights, which are non-transferable, author's rights may be assigned or licensed, but solely with the express consent of the owner. Free licences are "non exclusive" and cannot "strip" the ownership of the soft-ware from their creators. Free licences subject to copyleft do compel licensees to use the same licence (non exclusive) in any future distribution of modifi-

cations or work derived from the original software with these licences and to publish the relevant source code, as a condition of the right to redistribute the modification, but do not force them to "assign the software" (or their rights thereupon) to anyone.

5.1.4.   Free software cannot be subject to commercial use

Another misconception: as we have seen, there are no limitations to the use of free software (freedom 0); the only conditions imposed, sometimes, refer to its subsequent modification and distribution. Free licences do not affect the end users.

5.1.5.   Free software and non-free software are incompatible

Another myth is that free software is incompatible with non-free software if they are run on the same computer system or platform. If this were true, no non-free application, such as the Oracle databases, could be run on GNU/ Linux, OpenBSD or the web Apache servers. And vice-versa, free applications such as MySQL could not be run on non-free operating systems such as Oracle's Solaris or IBM's AIX. What may give rise to incompatibilities is the integration or mixing of copyleft software and non-free software, as we shall discuss hereafter.

5.1.6.   Free software cannot be integrated or mixed with
non-free software

This claim holds that free software, in general, cannot be mixed or integrated with non-free software in the same application without affecting it and, accordingly, without breaching its conditions of user. A stronger way of expressing this is claiming that free software and GPL software in particular is viral and "infects" other applications: any application integrating GPL software becomes GPL software. This statement is partially untrue.

- Integration by end user. Free licences do not restrict the use of software with other applications: the possibility of its modification is a condition of its being free and there are no restrictions on its use. It is therefore necessary to distribute the source code with the object code or to make it available to the recipient. Nonetheless, any integration of free software (permitted by the free licence) with non-free software may be considered a modification of the integrated non-free software (if the source code is available to make it). Depending on the restrictions contained in the non-free licence, such modification could constitute a breach, regardless of whether the integrated program is free, non-free or redistributed. This is not a problem of the free software, but of the non-free software licence.

- Integration by an intermediary. Where restrictions may exist in relation to the integration of software of various types, whether free or non-free,

is with respect to its subsequent distribution. Permissive licences allow mixing and redistributing their software with non-free licences. On the other hand, *copyleft* licences prohibit redistribution with non-free licences of a "mix" of software with these non-free software licences, which practice has come to be known as the privatisation of free software. Certain free licences contain clauses seeking to partially allow this integration, such as the LGPL or the MPL, which we have discussed previously.

5.1.7. All free software is licensed in the same manner (upon the terms of the GPL)

There are substantial variations between the more than seventy free and open source software licences recognised by the OSI. When discussing licences, it is important to be much more careful in the use of the term free software, and distinguish between free licences in general, licences subject to copyleft and licences that are neither free nor open. It is important to clearly understand the terms open source, persistence or reciprocity and copyleft, which are characteristic of such free licences.

5.1.8. Free licences require the publication of modifications to the code

This is one of the most incorrect ideas propagated in respect of the workings of free licences. We shall distinguish between the position of end users and intermediaries (developers of programs for third parties):

- **End users**. Most free licences do not require that users should distribute their modifications or adaptations of free software (derived works, in legal jargon) or should publish them or contribute them to the development of the modified application. Some licences do require the latter, in some particular cases, solely in relation to corrections or modifications of the central code or kernel of the program. As we shall see, these obligations do not apply to additional elements added to the kernel or any extension of the application. Therefore, the end user shall not be required to publish their works based on free software.

- **Professionals and companies developing programs**. Those developing programs for clients are not required to distribute to the public (or to the original authors) any modifications to free software. What they are required to do is respect the original free licences, many of which require providing the source code to users or clients receiving them or, if only the object code is distributed, offering the source code to any third party (the GPLv2) or the recipient (the MPL, GPLv3) for a certain period. This is one of the requirements for using free software subject to copyleft.

> **Supplementary content**
>
> The Apple Public License 1.x required that any modification of the original program be sent to Apple and this was one of the reasons for it not being considered a free licence.

5.1.9. With free software there are no liabilities or warranties

It is necessary to recognise that this may be true, under current free software licences, especially when the software is distributed free of charge. Nonetheless, there are legal doubts in terms of the effectiveness of warranty disclaimers and liability limitation clauses, which may not be valid with respect to consumers, at least.

The myth, in reality, consists of thinking that non-free licences give greater warranties and accept a higher level of liability. Many non-free licences seek to limit the liability of the licensor (author or distributor) in terms quite similar to free software licences. Indeed, they usually seek to limit contractual warranties, for instance, to the repayment of the purchase price in case of a fault with the software is identified within a limit of ninety days.

Another argument regarding warranties and liability is that with virtual distribution systems over the internet, it is difficult to identify licensors and thereby claim any compensation. Many sites distributing free software, such as Sourceforge, are not the owners – licensors, or even "official" distributors similar to those who distribute proprietary packages.

Nonetheless, in some cases, such as that of the FSF or in businesses based on the distribution of free software packages such as Red Hat or Suse (Novell), there is an identifiable legal entity that could be subject to an action for liabilities if necessary. Furthermore, the obligation to maintain the copyright notice allows rightsholders of any component that could prove defective to be identified, even if they are not necessarily who distributed the program to the affected party.

In addition, free licences allow free software distributors to add warranty clauses (with or without an economic consideration), which is done with many packages destined for commercial distribution.

5.2. Some legal issues relating to the licences

After going over the myths surrounding the legal effects of free software licences, this section is intended to provide some practical comments on the legal issues of free software and free software licensing.

Besides technical and economic aspects, there are a variety of important legal issues to be considered so as to ensure the success of any activity involving free software, whether it be its creation and distribution or its implementation in public or private organisations, and it is highly recommended to establish the appropriate legal strategies.

Understanding broader legal issues relating to free software, such as the legal consequences of inbound licences or interrelations between various concepts we have discussed here (copyleft, compatibility, licensing regime, etc.), should help us to manage free software projects better and reduce perceived difficulties and FUD.

The subjects that we shall address in this section, the "practical effects" of free software licences, relate especially to the management of intellectual and industrial property in free software based projects. We will specifically comment on:

- How to choose a free licence.
- How to manage the contributions to free software projects.
- Compatibility between licences.
- Dual or multiple licensing.
- The effect of licences on free software forking.

5.2.1. Choosing a free licence

The terms of a free software licence to be applied to a project normally result from a compromise between several objectives, determined by the authors or team leaders (coordinators) of the project in question. Generally speaking, the following objectives are considered, which may to a certain extent conflict with one another:

- Guaranteeing certain basic freedoms common to all free software (use, copy, modification, redistribution, patents, etc.).
- Imposing some conditions or restrictions (recognition of authorship, absence of warranty, use of trademarks, etc.).
- Procuring that the modifications and derived works should also be free, or not.
- Reserving some rights.
- Maintaining control over the evolution of the program.

Each project therefore has its objectives and criteria in terms of the licence.

In general when choosing a license for a project, it is recommended to use an already-existing licence rather than writing a new one. This issue has become increasingly more important due to the proliferation of free software licences (to the point that the OSI is attempting to reduce the number of certified licences). A general trend is to rely on one of the more common licences: GPL, LGPL, BSD, MIT, MPL, Apache, CPL, etc. This offers the advantage of increasing compatibility probabilities between programs and components. Another possibility is to look to a "third generation" licence, such as the GPLv3, OSL 3.0 or EUPL 1.1 licences (copyleft/reciprocal), or the Apache 2.0 or AFL 3.0 li-

cences (permissive), which cover certain issues that have arisen recently, such as patents, trademarks, remote use over a network, etc. and, for our purposes, may be better suited to the European legal framework.

> Many free software exponents recommend the use of a licence compatible with GPL, especially as it is used by almost 75% of the free software projects (not necessarily 75% of the available free software), but also as GPL generally receives more support from the free development community. There is some controversy in this regard, inasmuch as there are projects and developers that refuse to accept GPL code and others solely accept code under GPL or a compatible licence.

The main criterion is usually whether a project wishes to impose copyleft or reciprocity obligations: the obligation for developments based on the original software, generally derived works, to maintain the same licence for redistribution. The GPL, for instance, seeks to enlarge the pool of free software available and maximise the freedom of end users: it therefore includes the copyleft clause. The GPL also has the practical effect of limiting forking (a separate evolution of the same software over various projects – see below). As we have seen, other licences such as the LGPL or MPL have a weaker copyleft effect, applied solely to the original work (or component) and to any specific modification. It does not extend to applications "integrating" or "using" the free component. These allow for the integration or linking of the original components with another code, to create what are known as "larger works".

> Some questions that are often considered include:
>
> - Do I wish to allow the privatisation of derived works and modifications?
> - Do I want the developers to return their modifications to the free community in general, or to me, the initial author, in particular?
> - Do I want to allow the licensees to merge or link their program to mine?
> - Do I want a greater dissemination of the program and to attempt to establish a standard?
> - Do I want to obtain licence fees from my program, based on its use (commercial or otherwise), while at the same time permitting free development?
> - Do I have a unique innovative program, or is it just another content management system, for instance, when there are already many of them available, both free and non-free?
> - Do I have obligations with third parties in relation to the code incorporated in my program?
> - Does my program need to be run with any other program in particular? Are there restrictions thereon?
> - Do I want to encourage other developers to participate in my project and contribute code or test hours?
> - Has my application been designed to be embedded into a device, along with other, non-free, software?
> - Is there a "predominant" licence in the sector of my particular software (for instance, a language or libraries)?
> - Is there any risk for anyone holding or applying for a patent on an element or an aspect of the program?

The following chart, which is already a "classic" and appears in almost all documents on the subject, takes into account the main free licences and assists in the selection of a licence.

Criterion Licence	Allows linking with non-free programs	Can be mixed with other software	Allows deriva- tive works to be non-free	Grants a patent licence
GPLv2/v3				Yes
LGPLv2/v3	Yes			Yes
MPL	Yes	Yes		Yes
BSD	Yes	Yes	Yes	(no)

Another option lies in the choice of a dual licence policy, which we shall discuss below. This system, in which the program is distributed with different licences (normally one copyleft, the other restrictive licence), allows income to be obtained based on the non-free version of the software, and collaborating with a "community" to improve the free program on the free version.

Additionally, if the program is modular, it is possible to use different licences for different components, provided they are compatible in relation to the communication mechanism used by the components (i.e. depending on the degree of integration).

Another strategy for client/server systems is the use of a free licence for the client and a non-free licence for the server.

Supplementary content

This is the licensing system used by MySQL and Trolltech/ Qt, among other companies, see below.

Suggested reading

- Zooko O'Whielacronx: Quick Reference For Choosing a Free Software License http://zooko.com/license_quick_ref.html.
- Bruce Perens: The Open Source Definition, en "OPEN SOURCES", p185.
- Donald K. Rosenberg: Evaluation of Public Software Licenses, online at http://www.stromian.com/Public_Licenses.html (last visited March 29, 2001).
- Frank Hecker: Setting Up Shop: The Business of Open Source Software, online at http://www.hecker.org/writings/setting-up-shop.html.
- Mike Perry: Open Source Licenses, online at http://fscked.org/writings/OpenSource.html.
- Brian Behlendorf: Open Source as Business Strategy, en "OPEN SOURCES".
- Rex Brooks: Open Source Licenses Overview, online at http://www.vrml.org/TaskGroups/vrmlipr/open_source_overview.html.
- Eric Kidd: A History of "Open Source", online at http://discuss.userland.com/msgReader$19844#19889 (Aug. 19, 2000).
- Estudio POSS / IDA (Unysis para la Unión Europea), pp60-65.
- The Mitre Corporation: Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense, Version 1.2, 28 Octubre 2002, p. 15.

5.2.2. Licences for contributions and authorship

An essential element that must be taken into consideration when managing the legal issues of a free project is that of contributions to the project. The history of Netscape shows the difficulties that one could face if required to choose to free one's software or change from one free licence to another.

The problems that could arise when accepting third party contributions include:

- Software obtained from an unsafe source (may have been copied).
- Software contributed with another licence (an incompatible licence).
- Software covered by pre-existing obligations, either by third-party licences or commitments binding the author-licensor (the problem faced by Netscape).
- Patents granted on an element of the code.

Contributors tend to contribute code under various legal instruments: the project licence, a licence compatible with that of the project or a more individualised assignment (an agreement on contributions). There is a debate about whether contribution agreements should be mere permissive licences or joint or full assignment.

For those in charge of the project, it is important to have sufficient rights to incorporate and distribute the contribution in the project code. On top of this, they may wish to have wide rights so as to be able to change the licence in the future (e.g. evolve from GPLv2 to GPLv3), and finally, take legal action to defend against breaches of IP rights.

Accordingly, there are projects that request contributors to grant a complete and exclusive licence to the entity coordinating the project (in Anglo-Saxon countries, an assignment) with warranties in respect of the ownership of the rights to the contribution and, eventually, a patent licence. This allows project coordinators to keep certain control over the outcome of a free project and protect themselves from the risk that the code have come from unsafe sources (for instance, copied from other software) or that any original author that has requested a patent on the software or, in the law of English-speaking countries, revoke the licence.

Other projects are happy taking contributions under the project licence or a compatible licence (often a permissive licence such as a three clause BSD or MIT) or under a non-exclusive contribution licence agreement.

5.2.3. Compatibility between licences

We have raised the issue code and licence compatibility on several occasions.

A program is legally compatible with another if their codes may be mixed so as to create a derived work (made up of elements of each) and you can distribute the result of the integration without infringing upon the licences of both – i.e. the conditions of both licences may be met when redistributing the results.

| **Supplementary content** |
| For those in charge of the project, it is necessary to follow carefully the code that is contributed and keep a log of authorship and versions, identifying each software component. |

| **Supplementary content** |
| The FSF usually demands that any programmer contributing more than ten lines of software to a GNU project should assign the code exclusively to the FSF. |

To distribute software integrating several free software components legally, it is essential that the licences on the components (inbound licences) be compatible with the licence chosen for the distribution of the final product (outbound licence). For instance, as the new (or three clause) BSD licence allows almost any form of exploitation of the associated software, BSD software may be mixed or integrated with other programs with almost any licence (the GPL, for instance) and the result may be distributed under such licence without infringing upon the BSD.

Licences with copyleft are incompatible among each other, except where specifically agreed (such as the EUPL, LGPL or AGPLv3, or multiple licensed MPL code). When redistributing a program integrating two components with different copyleft licences, the use of one of the licences for the distribution of the final product would constitute an infringement of the terms of the other.

Probably the greatest debate surrounding free software is the question of licence compatibility and linking: even if two programs cannot be integrated together as a whole (e.g. statically compiled together and linked to create the executable), could they be dynamically linked? This may be achieved in various forms, as we have discussed in relation to GPLv2: for instance, inserting an API between one component and another or creating dynamic links that activate when run.

> The MPL expressly provides that applications under other licences may be linked with or use software under this licence, as a larger work. Usually, the non-free program must be linked to the software under MPL by means of an API. The API would generally be part of the original program, or a customised modification, and will therefore be subject to the MPL, while the linking program can be licensed under any licence, even non-free.

5.2.4. Dual or multiple licensing regimes

As free software licences are non exclusive, a program may be distributed by its rightsholder under two or more free licences, or under a free licence and a non-free licence, under a dual licensing system. A rightsholder is not restricted as to licensing the code, unless an exclusive licence has been granted or, in certain cases, confidentiality agreements have been established.

> Several programs are distributed in this manner:
>
> - MySQL is a database engine distributed under GPL for independent use and with a non-free licence for integration with commercial products.
> - eZ-publish is an internet content management program that also has a dual GPL/non-free licence.
> - The MPL 1.1. allows the owner to establish whether the program is distributed with the MPL or other licences (Clause 13).

From the viewpoint of the software rightsholder, the possibility of using a second licence allows him/her to offer different solutions to different stakeholders: community members (free licence) or clients (non-free licence or free

Supplementary content

Several projects have strived to be compatible with the GPL, such as Python, Qt and Vim, and even Mozilla added an additional clause to permit dual licensing.

Supplementary content

The FSF offers a complex chart on the compatibility between the GPLv2 and the GPLv3, covering several cases. See the FSF site.

subject to restrictions). This also allows controlling the price, quality and liabilities with respect to the software on the commercial side, and, eventually, releasing it (as Sun has with the Java technologies).

To accomplish this strategy, in the case of using a non-free licence as a second licence, it is essential that the rightsholder ensures ownership of the rights in all components incorporated in the product, or at least that the licences on any third party components are permissive (BSD, MIT), thus permitting relicensing under many terms. Therefore, projects that dual license their products tend to centralise the author's rights in sub-components in their hands, as is done by companies such as MySQL AB and Trolltech.

> This requires community contributors to assign their rights to their contribution to the project, to ensure there is no parallel use of valuable contributions (or provide very wide contribution licence terms). Projects should also establish restrictive licences with commercial partners and control patent risk.

The success of the strategy depends on the likelihood of third parties (whether commercial or within the free software community) creating a similar product or fork, which would compete for the product with a non-free licence. The use of a copyleft licence for the free licence usually prevents third parties from taking the free program and privatising it for commercial purposes, competing with the commercial version with a non-free licence.

Another element for controlling software in the context of this strategy lies in trademarks, a legal tool that we have already discussed. Trademarks are used by the Apache Foundation with respect to its software (the web server, Tomcat, etc.), by Sun in relation to Java® and by several professional free software companies such as Sugar® (CRM), Compiere® and Openbravo® (ERP), Pentaho® (Business Intelligence), Alfresco® (document management) and Zimbra® (mail and groupware), Socialtext®, etc.

5.2.5. Free software licences and forking

The concept of forking or division comes from computer multitasking: it refers to the division of one task or process into two. For instance, a task may remain active while another is stopped. The division or forking of a program takes place when the software is modified and the modification is developed separately as a separate branch or project, under another coordination team, and is often distributed under another name and perhaps another licence. Examples of these are OpenBSD and NetBSD, divisions of the original Unix BSD, and Compiere and Adempiere, etc.

> MySQL defines forking as: "Forking [of MySQL] means to divide the source code of the MySQL database in a repository kept separately, so as any development of the original code requires a manual operation to be transferred to the forked software, or that the forked software begins to incorporate functions not present in the original software".

> The program that has suffered this phenomenon most is UNIX, leading to the creation of up to ten variants. Some UNIX variants were created because their original authors (AT&T and the University of California, Berkeley) distributed them under permissive free

licences, allowing new versions (even non-free) to be created: Unixware by Novell, Open Server SCO, Solaris by Oracle, AIX by IBM, etc. This has given rise to legal problems, for instance, in the original case between AT&T and the University of California, and more recently between SCO and IBM, and others.

The possibility of forking is relevant to developers, inasmuch as it provides an indication of the possible technical and legal or commercial evolution of the software. From a technical viewpoint, "forked" versions tend to be technically incompatible (or "non interoperable") with the original programs. From a legal and commercial viewpoint, these versions may compete with the original product and be distributed with a different licence, either free or commercial, fostering legal incompatibility.

There are several reasons for forking.

- Developers fork free software because they (legally) can: free licences allow the modification of free software and the redistribution of such modifications. For instance, the BSD licence allows derived works to be created from the original software and changing the licence on the modified code. The new program could start as a mere variant from the original (for instance, OpenBSD with regard to NetBSD) and then diverge more and more.
- Another reason lies in the management of the development equipment and in disagreements between the programmers or owners of the software (Mambo/Joomla, is an example). For instance, if the need for an extension or new module is identified and the coordinator does not agree, it is quite likely that someone may create a forked version to integrate such a module.

Free licences have a direct influence on forking:

- Generally speaking, free software licences enable forks: software subject to a non-free licence or shareware cannot be forked.
- Software licensed under terms that do not allow commercial use and/or demanding the return of the modifications to the original author cannot be forked due to the centralising control exercised by the author (for instance, Ghostscript and the Aladdin licence).
- Software under strong copyleft licences such as the GPL tend not to be forked: derived works must be made available to licensees under the terms of the same licence, and the original project may, therefore, usually have access to the derived code so as to reincorporate any improvement and make it part of its own version.
- Software with weak copyleft licences, such as the Artistic, the MPL or the LGPL may be forked more easily, as they allow the creation of non-free or free variants by "aggregation".
- Software under a permissive licence (BSD or similar) can and is easily forked, as it allows binary distributions without the obligation to publish

the source code, and therefore, the original project may not have access
to the changes made in the fork.

6. Conclusion

In this module, we have looked at software licensing in general and at the legal aspects of free software licences and licensing in particular.

There are currently "many" free licences and free licensing models. In fact, there are so many recognised licences (some seventy have been approved by the OSI as "open sourced") that the OSI has established a committee against licence proliferation, something that we comment upon here.

> On its website, the OSI has classified (arbitrarily, according to some) the available licences as "most popular", "special purpose", and "other" and "redundant". We have observed with interest on Sourceforge, the largest repository of free software, the evolution of the use of the various licences, with the GPLv2 still in the lead, accounting for some 65% of the projects (which does not necessarily imply 70% of the code).

However, software and licences are not created and used in a stable and invariable environment, but rather are immersed in a changing medium, evolving quickly, both technically and legally. For instance, dynamic linking and interpreted languages did not really exist when the GPL v.2.0 was drafted, nor was there legislation for the protection of rights management information and technological protection measures. Consequently, to maintain software freedom, both technology and the legal framework need to evolve together, e.g. by adapting licences to new technological developments (SaaS, web-services) and legal developments (DRM).

Supplementary content
We have seen that the ¡GPLv3 was drafted taking into account both technology and legal change, and the Mozilla project has just announced (March 2010) that it is starting a community process to review the MPL 1.1.

Also, we wish to stress the importance of understanding software licences, their choice and how to comply with their terms, in relation to the use, distribution and marketing of free software or products based on free software in increasingly-complex development and production environments, such as distributed environments (web-services, software as a service, etc.):

- For software developers it is also fundamental to manage their own intellectual property and that of the contributors of code to the projects they run.
- For users, it is important to understand the licences applied to the programs they use, the rights they enjoy and the obligations they must comply with, and the differences and compatibilities between licences.

Regarding the professional life of the student, we think that it is important that they be able to assess the commercial and technological consequences of the legal issues that we have described and commented on here: what may be done in relation to the legal effectiveness or ineffectiveness of licences, how to take advantage of the possibilities of multiple licences, what documentation

or checklists could be useful for IP management, what strategy or tactic must be adopted when facing legal doubts with respect to free software, and which decision process is most appropriate.

Legal aspects of online activities (Internet)

Universitat Oberta de Catalunya

www.uoc.edu

Index

1. Introduction

This module looks briefly at the regulatory framework of online activities, in both civil and criminal law areas. This topic has been written on extensively, indeed it would need a whole book (rather, several) to cover all the relevant issues and the objective here is just to provide an overview of key topics: internet governance, online service provider liability and the regulation of electronic commerce and digital signatures. We will also look briefly at the fight against cybercrime.

First, as an introduction, we briefly comment on the initiatives for the protection of "digital rights" and on internet governance.

Online reading

- WSIS bibliography at http://www.itu.int/wsis/documents/bibliography.html provides an interesting list of readings on this topic.
- Other online reading includes:
  - European Commission: http://europa.eu/pol/infso/index_en.htm
  - The Internet Society: http://www.isoc.org/internet/law/
  - EFF: The Internet Law Treatise http://ilt.eff.org/index.php/Table_of_Contents
  - Stanford University: http://cyberlaw.stanford.edu/
  - Harvard University: http://cyber.law.harvard.edu/
  - BILETA: http://www.bileta.ac.uk/default.aspx

- Journals:
  - JILT: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/
  - Int. Jnl. of Law and Info. Technology:
    http://www.oxfordjournals.org/our_journals/inttec/editorial_board.html

1.1. Digital rights

The term "digital rights" describes the rights of persons in respect of the use of computers or electronic devices, or a communications network. In particular, the concept of digital rights relates to the protection of existing rights, such as the right to freedom of expression or privacy, in the online world, i.e. in the context of new digital technologies.

The rights in question that are considered relevant in an online context include fundamental human rights such as freedom of expression, privacy and freedom of association; and certain other important rights like the right to education or consumer rights.

These issues have mainly arisen as the extension of digital technologies into our lives has modified a previously existing balance between the individual and the state, and between individuals. The main thrust of the initiatives and regulation has been to protect existing rights in the new context (free speech),

and create or develop other rights in relation to technology within the context of protecting basic human rights and dignity in the digital "panopticon" (digital anonymity).

To a certain extent, the extension of certain rights to the digital context is fairly evident. Take for example two areas: free speech and privacy.

- As the internet is basically a communication tool, the right to free expression or freedom of speech is obviously a major issue, and has given rise to a series of cases and declarations regarding journalist rights, individual's rights to self-expression (through web 2.0 technologies such as blogs, twitter, etc.), the defence of criticism and parody, and how to deal with online defamation.

- The massive use of information (and the opportunity to massively use and connect information) combined with certain monitoring or privacy invasive activities – from the simple webpage cookie to data scraping and harvesting from the web to real-time monitoring of activities (Carnivore, key logging, etc.), has impinged on individuals' rights to privacy. This has in turn led to , giving rise to greater use of encryption (and thus the government's desire to regulate encryption technologies and private keys).

Other issues are not so evident:

- The determination of where an activity takes place (e.g. publication of defamatory work), so as to decide where to take action to protect or defend one's rights.

- The right to anonymity (e.g. using TOR networks or other identity hiding systems) and access by government to cryptographic keys (e.g. see the EFF site).

- Digital rights management systems that monitor or control a person's use of certain technologies (e.g. Sony Rootkit matter).

- Behaviour tracking on the web (e.g. Google's email screening; see the Working Party 29).

- Travel screening (the US control on air passenger information, see the EPIC and the Statewatch sites).

- Misuse of "cease and desist" letters (letters requiring certain information to be taken down or an activity to stop, alleging infringement of intellectual property or other rights). While these C+D letters are a valid means for defending a person's rights such as privacy or IP rights, they have often

been abused so as to censure legitimate activities such as criticism, report-
ing or linking (see the Chilling effects site).

This is not the space to cover these issues in great details, as this course focuses
on technologies, however it is interesting to note that a series of initiatives
have been undertaken in this area, which provide interesting further reading:

- The **World Summit on the Information Society** (WSIS). These confer-
  ences were set up in 2003 and 2005 under the United Nations. This sum-
  mit was highly controversial (particularly regarding ICANN), aiming to
  provide a discussion forum and framework for the protection of rights in
  the digital environment, leading to significant negotiations between gov-
  ernments, businesses and civil society. This is an ongoing activity, and has
  currently lead to the WSIS Declaration of Principles, reaffirming human
  rights.

  WSIS Declaration of Principles

  The WSIS Declaration of Principles is a series of statements or principles aiming to estab-
  lish "an information society accessible to all and based on shared knowledge". There is
  an associated "Action Plan" to bring more than 50% of the world's population online by
  2015. The 67 principles affirm, among other things:

  - A commitment to build a "people-centred", inclusive and development-oriented In-
    formation Society.
  - The universality, indivisibility, interdependence and interrelation of all human rights
    and fundamental freedoms, including freedom of opinion and expression.
  - The sovereign equality of states (i.e. no interference with internal matters... such as
    censorship!).
  - The recognition of diversity, special needs, the need to support the poor, and the
    need of inclusiveness, partnership and cooperation among governments and other
    stakeholders.
  - To meet these challenges by:
    – improving access to information and communication infrastructure and tech-
      nologies;
    – providing access to information and knowledge;
    – building capacity and IT applications;
    – increasing confidence and security in the use of ICTs;
    – creating an enabling environment at all levels (legal, economic, social, standard-
      isation, etc.);
    – recognising the role of the media;
    – addressing the ethical dimensions of the Information Society; and
    – encouraging international and regional cooperation.

  Work is ongoing, within the context of the "WSIS follow up" and the Tunis Agenda.

  One interesting aspect of WSIS from a technological point of view is the One Laptop
  Per Child initiative of Nicholas Negroponte, chairman and founder of the Massachusetts
  Institute of Technology Media Labs. This initiative was first presented at the WSIS and
  the objective was to present, at the 2005 Tunis meeting, a 100 USD laptop (running
  GNU/Linux, of course).

- The **Global Network Initiative** (GNI). This initiative was founded with a
  stated objective of "Protecting and advancing freedom of expression and
  privacy in Information and Communications Technologies". This oddly
  enough includes a series of a multi-stakeholder group of companies, civil
  society organisations (including human rights and press freedom groups),
  investors and academics. These parties spent two years negotiating and
  creating a collaborative approach to protect and advance freedom of ex-

pression and privacy in the ICT sector. They have developed Principles and Guidelines and Governance charter for this purpose, to provide direction and guidance in relation to the use of ICTs.

The GNI Principles and Guidelines and Governance

The GNI principles are aimed at defending freedom of expression and privacy in ICTs, basically stating that ICT companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. The principles are based on the Universal Declaration of Human Rights and other international documents, and cover the following issues:

- Freedom of Expression. On top of the generally accepted principal of free speech and absence of government restrictions, the principles recognise that broad public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential.
  Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimise the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.
- Privacy: this is stated as a human right and guarantor of human dignity, important to maintaining personal security, protecting identity and promoting freedom of expression.
  Participating companies will employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users.

To implement these principles, the guidelines focus on:

- Responsible company decision making: integration of the principles into company management and culture.
- Multi-stakeholder collaboration: development of collaborative strategies involving business, industry associations, civil society organisations, investors and academics.
- Governance, Accountability and Transparency: implementing a governance structure and demanding accountability through transparency and public scrutiny.

- **European Digital Rights** (EDRi) is an international advocacy group founded in 2002 by members from several European countries to defend civil rights in the information society. This group monitors regulation regarding the internet, copyright and privacy in European and International institutions. They have covered data retention requirements, spam, telecommunications interception, copyright and fair use restrictions, the cyber-crime treaty, rating, filtering and blocking of internet content and notice-and-takedown procedures of websites.

- The **Electronic Frontier Foundation** (EFF) is an international non-profit digital rights advocacy based in the United States. Its stated mission is to defend free speech, privacy, innovation, and consumer rights online. EFF was one of the early players in defending digital rights, helping educational activities policy-makers (e.g. with regard to free and open telecommunications networks), raising public awareness about civil liberties issues arising from the rapid advancement in the area of new computer-based communications media; and, interesting from a legal perspective, supporting litigation to protect these rights. Among other issues, they have been active with regard to:

- P2P Technologies (MGM v. Grokster, INDUCE Act).

- Online journalism and defending the confidentiality of sources (Apple v. Does).
- Privacy protecting technologies (Bernstein v. U.S. Dept. of Justice).
- Online censorship (ACLU v. Reno / Communications Decency Act).

MGM v. Grokster

The content industry has been fighting against online peer-to-peer P2P file-sharing systems since Napster, in 1998. Their arguments are that these systems infringe the IP rights of the content holders, inducing and actually committing breaches of copyright. However, since the Sony v. Betamax case of 1984, the US courts have held that a company is not liable for creating a technology that some customers may use for copyright infringing purposes, so long as the technology is capable of substantial non-infringing uses. P2P file sharing systems themselves, while permitting users to share copyright protected works, are also used to distribute works under free content licences and works in the public domain. Napster was shut down (in the end, voluntarily) because the centralised system did in fact contain the works that were being shared, and thus the system itself was infringing IP rights. In the Grokster case, "Hollywood" sued Grokster, a distributor of the file-sharing software. In this case, Grokster itself never actually reproduced the shared works in its systems – just provided a mechanism for sharing the links. After lengthy legal battles, the courts did not overturn the Betamax doctrine, however found Grokster guilty of "secondarily liability" for IP infringement (i.e. not directly committing the act, but "inducing" it), stating that it actively promoted illegal file sharing, did not implement any filters on content passing through its systems, and built a business model based on the use of third party protected works.

Apple v. Does

In 2004, Apple took legal action against unnamed individuals who allegedly leaked information about new Apple products to several online news sites, in particular concerning a FireWire audio interface. Apple also filed a separate trade secret suit against a site called Think Secret in 2005. Apple sought the identities of the persons who had leaked the information to the journalists of these sites. EFF successfully defended the journalists and sites in question against revealing their sources, on the basis of the confidentiality of media sources.

Bernstein v. US Dept. Justice

In 1995, Daniel Bernstein, a Berkeley university researcher, planned to distribute an encryption program he had written (called Snuffle) that could help prevent third parties from intercepting online communications, discovering passwords and, for example, stealing credit card numbers. US laws (export control and traffic in arms regulation) restricted the publication of his program, as encryption technology falls within weapons control laws (Waasemar treaty), treated as a potential threat to national security. The US federal courts affirmed, for the first time, that software code deserves First Amendment (free speech) protection and thus Bernstein could publish the code and scientific papers about the algorithm.

ACLU v. Reno

In 1996, the US promulgated the Communications Decency Act, a law in favour of Safe Internet and criminalising the publication of certain content online (that the government could not prohibit offline). EFF and a group of interested parties (ACLU being one of them) questioned the constitutionality of the law and the Supreme Court eventually declared it unconstitutional on the basis of the protection of free speech. US Congress then passed the Children Online Protection Act (criminalising "commercial" distribution of material deemed "harmful to minors") and the courts have granted orders against its enforcement, basically for being too wide in scope.

- The **Open Rights Group** (ORG) is a UK-based organisation campaigning on digital rights issues and online freedom, and acts as a media clearinghouse service putting journalists in touch with experts, "*fostering a community of grassroots activists*". It campaigns against digital rights management (DRM), the extension of the term of copyright protection afforded to sound recordings, e-voting, as well as numerous other issues.

Other interesting organisations to follow include:

- **Statewatch** "monitoring the state and civil liberties in Europe".

- **European Civil Liberties Network** (ECLN) "seeking to create a European society based on freedom and equality, of fundamental civil liberties and personal and political freedoms, of free movement and freedom of information, and equal rights for minorities".

- **Electronic Privacy Information Center** (EPIC) "Focusing public attention on emerging privacy and civil liberties issues".

- **Foundation for a free information infrastructure** (FFII) "information about free and competitive software markets, genuine open standards and patent systems with lesser barriers to competition".

1.2. Internet governance

One topic that gave rise to significant concerns at the origins of the internet is the technology governance model (i.e. who regulates the communications network). While it is still an issue, it has gone off the agenda more recently, as other "hot topics" such as "content piracy" or "digital terrorism" have arisen.

Originally, the internet was a private (academic) and US-centred network, and governance was established on a closed model, carried out by engineers and scientists. The private sector provided a significant amount of the investment and infrastructure (the international backbone infrastructure, the national cable networks, and provides services that facilitate and manage traffic).

As regards communications standards and the technological operation of the internet, the IETF (Internet Engineering Task Force), a private body, developed certain technical rules for the functioning of the internet (protocol definition, etc.). They were reinforced by the W3C (world wide web consortium) defining standards and protocols for that part of the internet that is the world wide web.

However, overall, a key element of the network has been the resources for network names and addresses: domain names, IP addresses. Originally, the IANA (Internet Assigned Numbers Authority) was responsible for assigning internet names and addresses. However, the American government decided, in the late 1990s, to contract some of the services provided by IANA from ICANN (the Internet Corporation for Assigned Numbers and Names).

ICANN is a US non-profit public-benefit corporation and is responsible for coordinating the management of the Domain Name System (DNS), the allocation of internet protocol address spaces, the coordination of new internet

coordination parameters and the management of the internet's root name server system. While ICANN is a quasi private organisation, it is assisted and monitored by a Governmental Advisory Committee (GAC) which is open to all governments and a number of international organisations with a direct interest in ICANN policy, including ITU, WIPO, OECD, etc.

- **Domain names**: Domain names are names by which internet hosts may be easily identified, as opposed to the numerical IP addressing system used for network communication. ICANN set out two types of registry:
  - a number of generic top-level domains (gTLDs), such as ".com", ".net", and ".org" which are used worldwide (expanded to .biz, .info, etc.);
  - about 240 national or territorial registries maintain similar systems of names under a country code (ccTLD registries), such as ".uk", ".fr".

  National registrars were set up for the ccTLDs (Nominet, ES-NIC, etc.) and ICANN accredited a number of private registrars (like Verisign) for registering domain names.
- **UDRP** (Uniform Dispute Resolution Policy) is a process established for the resolution of issues regarding the registration and use of domain names, supervised at an international level by WIPO, and at national level by the corresponding registrars. We have commented on this issue in the module on trademark use on the internet.

While ICANN argues it has succeeded in maintaining the stability of the Domain Name System for ten years now, and encouraged a participative decision-making process, there have been a series of criticisms concerning its private nature, its lack of representativeness and even its monopolistic tendencies.

- The legal structure and incorporation of ICANN under Californian law poses problems, including conflicts of applicable law and jurisdictions.
- Legitimate concerns remain as to whether a governmental committee advising a private corporation is an appropriate and effective mechanism to enable governments to exercise their public policy responsibilities.
- On top of this, the self-regulatory approach as practised by ICANN means that incumbent operators play a potentially inappropriate role (e.g. from the standpoint of competition policy) in setting entry conditions for new competitors.

For further information on the topic, see an early article[1] and contrast with information at Icann Watch, GIPI and IGF.

[1]For example, at the Duke Law & Technology Review.

2. Online activities

We consider that it is important to have minimum knowledge of the rights and obligations regarding online activities, particularly in respect of internet related services (access, hosting, linking, etc.) and web platforms, both those that merely broadcast information ("passive" sites) as well as those of electronic commerce (dynamic sites), and the most recent social networks (Facebook, YouTube, Flickr, Twitter, etc.).

There has been a significant amount of legislation to adapt the legal frameworks of the "analogue world" to the digital world, the "Information Society". This has mainly occurred at regional (i.e. European) level, to harmonise laws between member states of the EU so as to remove barriers against electronic trading: both providing information society services, and online contracting.

- Applicable regulation in this area at EU level includes:
  – 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. (Ecommerce Directive).
  – 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 (Copyright in the Information Society Directive).
  – 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 ("Distance Selling Directive").
  – 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 (Privacy Directive).
  – Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (IPR Enforcement Directive).

We have presented and commented on the last two Directives in the module on Intellectual Property Rights.

2.1. Information society services

The services supplied by the "*Providers of services of the information society*" are basically regulated on a European Level by the Electronic Commerce Directive, transposed nationally through various laws such as the Spanish "Ley de

los Servicios de la Sociedad de la Información y el Comercio Electrónico" or the English Electronic Commerce (EC Directive) Regulations 2002, Consumer Protection (Distance Selling) Regulations 2000.

In this section we will consider the administrative and legal framework for the provision of services (the scope of application of the regulations, administrative requirements and the legal regime applicable to international transactions) as well as the obligations that are binding for providers. In the following section, we will comment on electronic contracting and the regulation of commercial activities over the internet.

Online privacy issues are covered in the module on privacy.

The definition of information society services already exists in Community law in Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society; this definition covers "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".

Thus basically the Ecommerce Directive applies to all activities carried out by electronic means and having a commercial nature or pursuing a financial objective (to obtain financial income directly or indirectly). In other words, it applies to web pages that carry out electronic commerce activities as well as to those that supply information or offer services free for users, when they represent an economic activity for their owner.

The Directive and national laws cover both services between enterprises (B2B) and services between enterprises and consumers (B2C), as well as services provided free to the recipient (depending on the country, these may need to be financed, for example, by advertising income or sponsoring).

Information society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering online information or commercial communications, or those providing tools allowing for search, access and retrieval of data.

It covers the all sectors and activities, including in particular: newspapers, databases, financial services, professional services (solicitors, doctors, accountants, estate agents), entertainment services (video on demand, for example), direct marketing and advertising and Internet access services.

2.2.　Country of origin rule and applicable law

In an international environment such as the internet, it is important to determine the act that applies to the provision of a service. Otherwise, providers of services over the internet could be exposed to the control and applicable act of all the countries of the world. In order to avoid this problem, on a European level it has been ruled that, in most cases, the place where the service provider is established will determine the act and competent authorities that regulate them (the "country of origin" principle).

Thus under Article 3 of the Directive, providers of information society services are subject to the legislation of the Member State in which they are established. The Directive defines a provider's place of establishment as the place in which a service provider effectively pursues an economic activity using a fixed establishment for an indefinite period. Thus service providers established in France only need be concerned by French regulation, service providers established in Spain comply with Spanish laws, and so on (subject to what we mention below as to applicable law and jurisdiction, especially as regards consumers).

It is important to note that the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider. So a UK based service provider with equipment in France would not a priori be subject French regulation of its activities (except as regards consumer sales directed at France, see below).

2.2.1.　Applicable law and jurisdiction

Another area of doubt is which law applies to online relations and which courts should solve differences (in the event of international issues). This has always been a difficult issue, an area of law called Private International Law or Conflict of Laws.

With regards to electronic contracting, in general the law and competent courts agreed in the contract will apply. Failing that, the standard rules of Private International Law will apply. With contracts between consumers and professionals – the applicable law is that of the country of residence of the consumer, provided that this is also the country where the professional carries out his/her activities or to which his/her activities are directed. The parties may also, based on freedom of choice, apply another law, as long as it provides the same level of protection to the consumer as that of his/her country of residence (This is why, for example, consumer product distribution platforms are often customised for each target country – for example www.pixmania.com).

As regards non-contractual obligations and liabilities (torts, IPR issues, etc.), the "Rome II" convention (since 2009, Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations) provides that the applicable law is:

- The law of the country where the damage occurs.
- The law of the country where both parties were habitually resident when the damage occurred.
- The law of the country with which the case is manifestly more closely connected than the other countries (using the "points of contact" doctrine").

As regards the courts that would hear any conflict ("jurisdiction"), this is also covered at European level and case law. Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (as amended) provides that:

- The basic principle is that jurisdiction is to be exercised by the Member State in which the defendant is domiciled, regardless of his/her nationality. This will always be the case for consumer defendants.
- Apart from the basic principle on jurisdiction, in certain circumstances a defendant may be sued in the courts of another Member State, including: (IPR issues, other).
  - Contracts: where the parties have agreed or where the obligation is performed.
  - Family maintenance: where the creditor (the person paying maintenance) is domiciled.
  - Torts (wrongful acts): where the harmful act occurred (including IP infringement).
  - Consumers: always in their own domicile (see next).
  - Insurance: where the insurer is domiciled.

- In order for the consumer to enjoy this protection in his/her home domicile in other cases, the consumer contract must have been concluded with a person either who pursues has commercial or professional activities in in the Member State in which the consumer's Member State (e.g. a local or national business), or is domiciled this company/professional "or directs" such these activities to that Member State (e.g. a business is domiciled in the UK, but has an online platform for selling products across the rest of Europe, including e.g international delivery, and the website is in several European languages; in this case, the consumer can argue that the platform is directing its activities at the consumer in another country).
- A consumer may either bring proceedings either in the courts of the Member State in which the defendant is domiciled or in the courts for the place where the consumer (as plaintiff) is domiciled.

2.3. Service Provider obligations

In order to provide services over the internet, companies do not need to request authorisation or sign any registry. However, with a view to improving the transparency of "remote" commerce, service providers are obliged to publish certain data about themselves and their products.

- **General information obligations**. Service providers must indicate on their web page:
  - Their company name and contact details (address, email address and any other detail allowing direct and effective communication, for example a telephone or fax number).
  - If the company is inscribed in the Company Register or any other public register, stating also the corresponding inscription number.
  - The company's tax identification number (for VAT purposes).
  - Information regarding product prices, whether or not they include applicable taxes, delivery costs, and any other data that ought to be included under applicable norms of the autonomous communities.
  - Details regarding any administrative authorisation where necessary, as well as the relevant supervisory body.
  - Details of the professional body for regulated professions (Lawyers, attorneys, doctors, etc.), and the affiliation number, academic qualification and State of the European Union that issued it with the corresponding approval where applicable.
  - Codes of Conduct adhered to, where applicable, and the means of consulting them electronically.

- **Obligations regarding cookies and security**. The use of *cookies* is not prohibited, since they are sometimes necessary in order to facilitate communications or to customise websites, however, as a modification to the original Directive, service providers must provide clear and complete information on the use and purpose of *cookies*, offering the possibility of rejecting the processing of data through a simple and free procedure (basically, by deactivating them in the browser).
  At the same time, *internet access suppliers* are obliged to inform their users (for example, on their main web page or site), about:
  - the technical measures that ensure protection against security threats over the internet (computer viruses, spyware, spam),
  - tools for filtering unwanted content,
  - security measures applied in the provision of their services (together with email service providers),
  - potential liabilities that could be incurred through use of the internet for illicit purposes.

- **Additional obligations to collaborate and liability of intermediate service providers.** There is also an additional provision, articles 15 and 19, requiring member states to ensure the service provider supplies (and

thus collaborates with) national authorities (administrative and police) with "requisite information", specifically regarding alleged illegal activities, when so required , e.g. in order to interrupt the provision of a service or to identify an online user.

However, the law releases from liability certain internet "intermediaries"– access, data transmission, hosting and search engine services – with regards to the contents that they host, transmit, provide access to or classify in a link directory (see below). They are not obliged to supervise said content, for example. But they can be liable if they take an active part in its preparation or if, knowing that particular material is illegal, they do not act speedily to remove it or to prevent access to it.

3. Liability of information society service providers

Not all of the information transmitted through the internet is in compliance with national legal systems. The dissemination of some information is unlawful, e.g. images related to child pornography or works protected by intellectual property rights (for instance, the online publication of music or video works without authorisation). The diffusion of such content interferes with public or private interests.

The legal responsibility is borne by the authors of the online publications. Nonetheless, the question of intermediaries on the communication networks arises. Those intermediary players serve to transmit and host information and to provide access to a communication network (ISPs – Internet Service Providers).

The intermediaries do not have real control over all the information transmitted through their equipment. It would be expensive and technically difficult. Furthermore, considering intermediaries liable could be prejudicial to the development of the internet.

For that reason, the Ecommerce Directive provides a balanced solution for the interests at stake and aims to end the growing differences between Member States' legislation and case law that were emerging on the liability of internet intermediaries.

The directive does not just apply to copyright infringement but is established in a horizontal manner, so that it applies to all kinds of illegal materials (including copyright, unlawful commercial practises, breach of privacy, criminal liability, etc.).

However, to benefit from the protections, the service provider must be an "intermediary" and, therefore, the information must be provided by the third party recipients of services and must be transmitted or stored at their request.

The European directive covers three categories of online intermediary activities, and different conditions must be fulfilled for each one.

3.1. Activities covered and conditions for liability limitation

This directive creates a system that prevents online intermediaries from being held liable for specific activities under certain conditions.

For the activities or intermediaries not covered by the directive, or for intermediaries that do not fulfil the liability limitations conditions, the Directive refers to the applicable national law of liability of Member States.

Primarily, the Directive prohibits member states from obliging ISPs to monitor the content of the data they process. However, to benefit from the exemptions, they must satisfy the conditions, on an ongoing basis:

- **Mere conduit:** A mere conduit is defined as "*a service provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.*" It refers, for instance, to the functions of an internet access provider or network operators. An intermediary engaging in mere conduct activity will not be liable for the damages caused by the information transmitted as long as it does not:
  - Initiate the transmission.
  - Select the receiver of the transmission.
  - Select or modify the information contained in the transmission.

The provider cannot play an active role in the transmission of information. Its role has to be limited to the technical process of operating and giving access to a communication network. The condition of not having modified the information does not extend to the technical manipulations enabling the transmission of information since these do not alter the integrity of the information contained in the transmission.

Thus, insofar as the provider has a passive and neutral role, it may not be held liable for the information transmitted through its equipment, either at a civil or at a criminal level.

1) Caching: Caching consists of "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request". Any intermediary provider that carries out a caching activity will not be held liable as long as it meets the following conditions:

- It does not modify the information.
- It complies with conditions for accessing the information.
- It complies with rules for updating the information, specified in a manner widely recognised and used by industry.
- It does not interfere with the lawful use of technology widely recognised and used by industry to obtain data on the use of the information.
- It acts expeditiously to remove or disable access to the information it has stored upon obtaining knowledge of the fact that:
  - The information at the initial source of the transmission has been removed from the network.
  - Access to it has been disabled.

–   A court or an administrative authority has ordered such removal or
    disablement.

In other words, the intermediary provider must stay neutral concerning the
content of the information.

2) Hosting activity: Hosting is defined as an information society service that
consists of the "storage of information provided by a recipient of the service
and at his request."

For instance, it includes the activities of the internet access providers who
provide space on a server in order to store their clients' websites and therefore
make them accessible on the internet.

To enjoy the liability limitation, the provider of hosting activities must:

•   not have actual knowledge of illegal activity or information and,
•   upon obtaining such knowledge or awareness, act expeditiously to remove
    or to disable access to the information.

Therefore, the intermediary providing hosting will be held liable if it is proven
that he had knowledge of the existence of unlawful information (for instance
by third party notification denouncing the existence of such information) and
did not remove it or disable access to it.

There are differences as regards implementation of these provisions, with
some national laws requiring effective knowledge of an illegal act through
court order (so that the ISP does not have to take a decision as to whether
some material is infringing or not) or through being served private notice (e.g.
a take-down notice).

3.2.   Other activities

Interestingly, certain national legislation has extended the ecommerce direc-
tive protections to other intermediary activities, namely linking and search
engines.

•   **Links**: Hyperlinks are at the base and origin of internet technology. They
    constitute technical mechanisms that, like pointers, permit a logical link
    to be made between different hypertext contents, allowing for highly dy-
    namic browsing and obtaining of contents. While it is generally thought
    that no liability arises in respect of links created to infringing or illegal
    materials, unless "sponsoring" these materials, Spain for example has ex-
    plicitly excluded liability for links where the linker does not know of the

nature of the data to which he/she is linking and removes the link when he/she does have such knowledge.

- **Search engines**. Search engines like Google or Yahoo are also essential features of the net, enabling information to be found among literally millions of pages. Again, it is thought that search engines should not be liable for the content of the pages they link to as a result of a search, and specific exemption has also been given in the same conditions as for linking. This is not the case, however, for search engines "caches", when they fall outside the caching exemption commented above, as often these search engines themselves store old or removed (illegal) information and thus provide access to it.

Linking and other forms of internet features such as metatags in general have caused a series of case law and decision, with the courts approaching the matter in different ways. In particular, they have considered:

- **Linking** is generally held (Shetland Times) to be legal, provided the actual text o f the link itself is not a breach of tirad third party Rights (e.g. copyrighted work, such as – arguably – a newspaper title – see Shetland Times case, where a newspaper used the headlines of a competing newspaper to link to that paper, bypassing the front page.

- **Deep linking**: linking to a page that is not the "home" page of the linked site. Again this has been deemed to be licit, as it is understood that the whoel point of havinge "pages" is to be able to link to any of them, and the linked website owner has technical means for preventing linkers going direct to a sub-page.

- **Framing**: using a separate segment of the browser to display another company's linked webpage, not explicitly showing its URL – i.e. creating a frame round the linked site. This is generally understood to be a breach of the linked site owner's rights, if not unfair competition (where the linked content cannot be distinguished from the linker's own content, thus causing confusion). This is even more so when the framed content includes trademarks and other protected works.

- **Inlining**: creating webpages from third party content (stored on another site). Again, if the third party content is protected by copyright, it is generally considered to be illegal to "inline", at least when it is done without attribution. This is more controversial, for example, when search engines inline thumbnails or abbreviated parts of third party content. Again this is a technical issue, as the thumbnails or extracts themselves may not be inlined, but reproduced by the linking site.

- **Metatags** are a means of using certain data to mark up or inform on the content of a site. Certain sites will use trademarks and other protected signs to attract search engine attention (thus rising in the results ranking) – a practice which is generally considered illegal unless authorised by the rights holder or benefitting from other exemptions (fair use).

   For more reading: see Bechtold's page (updated to 2004 only) and more information at the Wikipedia site. Also commented at Bitlaw Legal Resource.

Bibliography

See for example http://searchenginewatch.com/2156551, comment at http://cyber.law.harvard.edu/property00/metatags/main.html and http://ilt.eff.org/index.php/Trademark:_Links,_Frames,_Search_Engines_And_Meta-Tags.

3.3. ISPs and IPR enforcement

While ISPs may benefit from exemptions with regard to the data they process on behalf of others, we have seen in the module in IPR that Directive 2004/48/EC on the enforcement of intellectual property rights (IPR Enforcement Directive), requires certain involved parties to provide information on the possessors of infringing products, the recipients of infringing services and those that have provided services to the infringer.

Thus in the field of e-commerce, the question may arise whether the intermediary service provider has the obligation to provide information on the recipients of its services (the infringers/the content providers carrying out illegal activities), or is exempted from such obligation by referring to the regulations on limitation of liability and exemption from monitoring obligation set out in Ecommerce Directive.

Under Article 8 of the Enforcement Directive, Member States must ensure that in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of a claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:

- Was found in possession of the infringing goods on a commercial scale.
- Was found to be using the infringing services on a commercial scale.
- Was found to be providing services used in infringing activities on a commercial scale.
- Was indicated by the person referred to in points (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.

The Enforcement Directive determines the scope of the information to be provided and regulations to be taken into account when enforcing the right to information – in particular, regulation as to the processing of personal data. So ISPs find themselves at the heart of a conflict between three laws (IPR, Privacy, Ecommerce).

ISPs are usually the target of IPR enforcement activities as they hold the data to identify users (IP address / domain name) and often host the allegedly illegal materials. Therefore, the question may arise whether the ISP has the obligation to provide information on the recipient of its service, the content provider committing infringement, or may be exempted from such obligation by referring to the regulations on liability limitation (Sections 7-13 of Ecommerce Directive) or the exemption from monitoring obligations (Section 7 (5) of Ecommerce Directive).

It is understood that the Enforcement Directive generally does not affect the principles of the Ecommerce Directive and does not at all affect the limitation of liability existing in favour of the intermediary service providers and set out in Articles 12-15. The introduction of the right to information is only compulsory in cases of illegal activities or services carried out on a commercial scale (for direct or indirect economic or commercial advantage; this would normally exclude acts carried out by end consumers acting in good faith). So that is already one area of comfort for ISPs.

However, it is also understood, on the basis of the recitals to the Ecommerce Directive, that limitations of the liability of ISPs do not affect the "possibility of injunctions of different kinds; such injunctions can, in particular, consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it." This is reinforced by information and collaboration obligations set out in national implementations of the Ecommerce Directive.

Thus it is not a question of _what_ ISPs have to do, but when and how: do they need a court order (so they are not considered to censure their user's content and breach privacy laws) or is it sufficient for a notice? This is an issue that is still unresolved, and will depend on how national laws are implemented and interpreted by courts.

So far, court cases vary (see L'Oréal –v– eBay in England, which has been referred to the ECJ), but on the whole intermediaries have escaped significant liability, e.g. in the recent Google Adwords case (Court of Justice of the EU, 23 March 2010, Cases C-236/08 to C-238/08). But IPR holders will not stop there.

4. Ecommerce – Online Contracting

Beyond the "information society service provider" information obligations
and ISP exemptions, the ecommerce regulations deal with electronic contracts
and online contracting, and oblige certain processes to be implemented for
the correct sale of products over the internet (presented in this section).

4.1. Valid electronic contracts

National laws pursuant to the Ecommerce Directive must guarantee the valid-
ity and effectiveness of contracts celebrated electronically, even if there is no
copy in paper format. In other words, a contract's electronic format is equiva-
lent to that written on paper and the effectiveness of electronic documents as
proof in court is reinforced (also admissible as evidence in court proceedings,
as we discuss below in relation to the electronic signature whereby electronic
signatures are equivalent if not better than manuscript signatures).

4.2. Information and processes

In order to guarantee the legality of the contracting process, on the basis of
the Ecommerce Directive and the Distance Sales Directive, service providers
must establish certain minimum processes:

- Before initiating the contracting procedure, the following information
  must be made available to the user, in a simple, free, clear, understandable
  and unequivocal manner:
  - The steps or processes to be followed in order to enter into the con-
    tract.
  - Whether the electronic document of the contract will be filed and
    whether it will be accessible.
  - The technical means made available in order to identify and correct
    errors in data input, before data is confirmed.
  - The language or languages in which the contract may be held.
  - The general conditions governing the contract, where applicable.

- Once the contract has been entered into, the provider must confirm re-
  ceipt of the contract's acceptance (by means of an acknowledgement of
  receipt by email or similar, or other equivalent means of communication
  to that used in the contracting process – sales confirmation screens, for
  example with an order or reference number).

  These electronic contracting processes can be verified on most e-commerce sites, for ex-
  ample, for the purchase of train or plane tickets, or downloads of commercial software
  (antivirus packages, etc.). They allow buyers to check the general conditions of the sale,

> **Supplementary content**
>
> It will be important to include
> these processes in the design
> (and budget!) of any interac-
> tive portal and the "back-of-
> fice" systems that support it.

and oblige them to accept these (ticking an "accept" check box) before confirming the purchase.

4.3. Obligations associated with remote selling to consumers

For the protection of consumers, national contract law may still affect B2C (Business to Consumer) transactions, which are deliberately not subject to country of origin principle: usually the national law of the consumer's country applies.

Luckily, consumer protection law is partly harmonised in the EU, including

- The Distance Selling Directive provides for the consumer's right to withdraw contracts and for different performance and credit card provisions.
- The Directive on unfair Terms in Consumer Contracts imposes the exclusion and limitation of liability.
- The Consumer sales and guarantees Directive establishes minimum levels of guarantees.

There is on the table a proposal to review and consolidate EU consumer protection laws.

In particular, the framework provide for:

- The provision of comprehensive information before the purchase.
- Confirmation of that information in a durable medium (such as written confirmation).
- Consumer's right to cancel the contract within a minimum of 7 working days without giving any reason and without penalty, except the cost of returning the goods (right of withdrawal).
- Where the consumer has cancelled the contract, the right to a refund within 30 days of cancellation.
- Delivery of the goods or performance of the service within 30 days of the day after the consumer placed his order.
- Protection from unsolicited selling.
- Protection from fraudulent use of payment cards.
- Non-validity of any waiver of the rights and obligations provided for under the directive, whether instigated by the consumer or the supplier.

Some types of contracts are excluded from these obligations, including contracts for financial services and contracts concluded through an auction (NB: contracts for financial services are covered by the Distance Marketing of Financial Services Directive 2002/65/EC.).

4.4. Commercial communications and publicity

Finally in the area of ecommerce, laws have set out provisions regulating "commercial communications" – "spam", when unsolicited (Art 7 Ecommerce Directive, as updated by Privacy Directives). These require the addressee's prior consent, both for email as well as for mobile messages. Nevertheless, the sending of commercial communications to those users with whom there is a previous contractual relationship is allowed, in which case the provider may send publicity regarding similar products or services to those contracted by the client.

For the protection of users, the provider must offer the addressee the possibility of opposing the processing of his data for promotional purposes, both at the time of collecting the data as well as in each commercial communication addressed to him. This option tends to be hidden in the general conditions of sale or subscription, which the user accepts when registering or confirming a purchase over the internet. The service provider must establish simple and free procedures for this purpose, as commented below in the section on data protection.

For the purpose of maintaining transparency and protecting the consumer, electronic publicity (emails, web pages, "YouTube" videos) must be presented as such, so that they cannot be confused with any other type of content, and clearly identify their nature to the advertiser.

Promotional offers (in other words, those that include gifts or prizes, or discounts, and competitions, or promotional games, etc.) must be clearly identified as such and the conditions of access and participation must be easily accessible and expressed in clear and unequivocal terms.

5. Electronic signatures

One of the areas of work of legislators over the last 10 or more years has been the use of electronic signatures and documents, to replace written signatures and paper copies of contracts, administrative forms and other commercial and administrative "documents". The basic framework at European level is Directive 1999/93/CE of the European Parliament, of 13 December 1999 establishing community framework for electronic signatures.

At this level, the regulations state that whenever certain minimum requirements are met in relation to the certificates, **then equivalent legal effectiveness is given to the electronic and handwritten signatures**. The Directive goes on to establish the criteria for legal acknowledgement of the digital signature, focusing on the services of certification.

These include:

- Common obligations for certification service providers in order to secure transborder recognition of signatures and certificates throughout the European Community.
- Common rules on liability to help build confidence among users, who rely on the certificates, and among service providers.
- Cooperative mechanisms to facilitate transborder recognition of signatures and certificates with third countries.

5.1. Electronic signatures

The Directive defines various forms of electronic signatures:

- **The electronic signature**, being data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. This could be an email signature.
- **The advanced electronic signature**, which meets the following requirements:
  - It is uniquely linked to the signatory.
  - It is capable of identifying the signatory.
  - It is created using means that the signatory can maintain under their sole control.
  - It is linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.

- **The qualified certificate, which must in particular include:**
  - An indication that it is issued as a qualified certificate.
  - The identification of the certification service provider.

–   The name of the signatory.

–   Provision for a specific attribute of the signatory to be included if rel-
    evant, depending on the purpose for which the certificate is intended.

–   Signature-verification data corresponding to signature-creation data
    under the control of the signatory.

–   An indication of the beginning and end of the period of validity of
    the certificate.

–   The identity code of the certificate.

–   The advanced electronic signature of the issuing certification service
    provider.

The certificate must also be issued by a certification service provider, which
meets specific requirements laid down in the Directive, establishing minimum
requirements for recognition across Europe.

To guarantee pan-European market access and recognition of signatures, the
Directive prohibits Member States from making the provision of certification
services subject to prior authorisation of any kind (they may introduce or
maintain voluntary accreditation schemes aimed at enhancing levels of certi-
fication-service provision), nor may they limit the number of accredited cer-
tification service providers for reasons which fall within the scope of the Di-
rective; nor may they restrict the provision of certification services originating
in another Member State in the areas covered by the Directive.

5.2. Legal effects of electronic signatures

The main provision of the Directive states that an advanced electronic signa-
ture based on a qualified certificate created by a secure-signature-creation de-
vice satisfies the legal requirements of a signature in relation to data in elec-
tronic form in the same manner as a handwritten signature satisfies those re-
quirements in relation to paper-based data (for convenience this type of sig-
nature is usually called a "qualified signature". It is also admissible as evidence
in legal proceedings.

In addition, an electronic signature may not legally be refused simply because:

•   It is in electronic form.

•   It is not based on a qualified certificate.

•   It is not based upon a qualified certificate issued by an accredited certifi-
    cation service provider.

•   It is not created by a secure signature-creation device.

Spain had legislated on the electronic signature in 1999, but came back to it in 2003 to
adapt the regulation and transpose the directive mentioned above in Act 59/2003, of 19
December, on the electronic signature. The latter regulates the legal effectiveness of the
electronic signature and the provision of certification services.

More recently, Act 56/2007, of 28 December, on Measures to Promote the Information Society modifies some precepts of the Act 59/2003, incorporating a new obligation for the Public Administration and certain companies, which entails the use of recognised electronic signature certificates in relations with citizens and clients, respectively.

6. Cybercrime

The growth of the Information Society has been accompanied by new series of crimes and misdemeanours, either directly against information society technologies (e.g. denial of service attacks, etc.) or using these technologies to commit traditional crimes such as fraud. The ITU believes that attacks against information infrastructure and internet services now have the potential to harm society in new and critical ways, due to the fundamental importance that these services and networks acquire in today's society and economy. Online fraud, the dissemination of child pornography and hacking attacks are just some examples of computer-related crimes that are committed on a large scale.

6.1. Introduction

The legal, technical and institutional challenges posed by the issue of *cybercrime* and its counterpart, "cybersecurity", are global and far-reaching, and it is thought and has been argued that it can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

Certain steps have been taken, both in the policy and the legal arenas. As regards policy, for example, the World Summit on the Information Society (WSIS) recognised the risks posed by inadequate cybersecurity and included it on its agenda in the 2003 and 2005 conferences. This led to the ITU setting up the Global Cybersecurity Agenda (GCA) in May 2007, a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity. Among the GCA work areas, the work on "*Legal measures*" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.

Due to the "novelty" of cybercrime (compared with crimes such as murder or theft), dealing with it requires first of all the necessary substantive criminal law provisions to criminalise acts such as computer fraud, illegal access, data interference, digital copyright violations and child pornography. Note that the fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network (e.g. creation or distribution of child pornography in paper format), does not mean that they can be applied to acts committed over the internet as well, because of the strict interpretation of criminal law.

> The computerisation of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago. The effective prosecution of these acts

requires that existing criminal law provisions not only protect tangible items and physi-
cal documents from manipulation, but also extend to include these new legal principles.

Then, once the crimes are defined, by substantive criminal law provisions, law
enforcement agencies need the necessary tools and instruments to investigate
cybercrime, using the same tools that the perpetrators use.

On a wider scale, the concept of "safe internet" has been used to cover the
attempts to make the internet safer (and protecting internet users) and has
become integral to the development of new services as well as governmental
policy. Initiatives in this area are both public (e.g. the European Commission
work) and private (e.g. Safe Internet Alliance).

6.2. Definitions and typology of cybercrime

One of the first difficulties has been the definition of "Cybercrime". Consid-
erable difficulties have arisen in defining the term, but a general consensus
is building towards it being defined as "any activity in which computers or
networks are a tool, a target or a place of criminal activity" or "computer-me-
diated activities which are either *illegal or considered illicit* by certain parties
and which can be conducted *through global electronic networks"*.

> See Convention on Cybercrime – Council of Europe Convention on Cybercrime (CETS
> No. 185).

Once we have a definition, we can study what activities specifically fall within
the concept and see the measures that have been taken against them.

To assist in understanding the scope and scale of cybercriminal activities, a use-
ful starting point is the Council of Europe Convention on Cybercrime (2001),
being an International Treaty signed and ratified by most European countries
and with additional parties such as USA, Canada, Japan, and Mexico. This
Convention distinguishes between four different types of offences, set out in
the following table:

Category	Specific crimes
Offences against the confidentiality, integrity and availability of computer data and systems	Illegal Access (Hacking, Cracking)
	Data Espionage
	Illegal Interception
	Data Interference
	System Interference
Content-related offences	Erotic or Pornographic Material (excluding Child-Pornography)
	Child Pornography
	Racism, Hate Speech, Glorification of Violence

Category	Specific crimes
	Religious Offences
	Illegal Gambling and Online Games
	Libel and False Information
	Spam and Related Threats
	Other Forms of Illegal Content
IPR-related offences	Copyright-related Offences
	Trademark-related Offences
Computer-related offences (offences that need a computer system to be committed)	Fraud and Computer– related Fraud (e.g. auction fraud)
	Computer-related Forgery
	Identity Theft
	Misuse of Devices (Carry out DoS attacks, designing and distributing computer viruses, Decrypt encrypted communication, Illegally access computer systems)

Obviously, there is significant disagreement between countries or areas with different cultures regarding the illegality of certain activities: while there is general agreement that child pornography should be prevented in all forms and manners, adult pornography is generally acceptable in most western societies. But within these, for example, there are significant different views on gambling, racism and hate speech (witness France and Germany's prohibition of any defence or promotion of Nazism, whereas USA tolerates this under its Freedom of Speech principles).

In Europe, child pornography in particular has had additional legislation, among others:

- The European Union Council Framework Decision on combating the sexual exploitation of children and child pornography (2003).
- The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007).

On the other hand, gambling for example has widely differing regulation over and outside the internet and the effect of different regulations is evident in success of "off-shore" gambling countries (Malta, Bahamas, UK...).

6.3. Technical and legal challenges

A number of challenges to creating an efficient international framework and process for dealing with cybercrime have been identified, most of the posed by the very technologies that underlie the Information Society:

- **Reliance on ICTs**: the greater the reliance our society has on ICTs, the more vulnerable it is to widespread attacks and the greater the impact.

- **Number of Users**: the increasing number of ICT users makes it increasingly difficult to identify criminals ... and increasingly easy for them to identify targets.

- **Availability of Devices and Access**: cybercrime was not really a public issue until personal computers and access to global networks became widespread, and with new and more sophisticated devices (mobile phones, "pads", etc.) and the pervasiveness of computing (home, office, etc.).

- **Availability of Information**: the global networks have given rise to easy access on topics such as how to make a home-made bomb, how to write computer viruses, etc.

- **Missing Mechanisms of Control**: the internet has no global regulator other than for technical reasons (DNS), which makes it difficult for authorities to exercise their powers.

- **International Dimensions**: Police forces and judicial authorities have local, regional or national jurisdiction, and processes for pursuing criminals across digital borders have not adapted with the speed of the networks.

- **Independence of Location and Presence at the Crime Site**: crimes may be initiated in one place, cause damage in another and the criminal may be located in a third (e.g. online publication by a person in France on a UK web-server that is defamatory to a person in Spain).

- **Automation and speed of data exchange processes**: automation speeds up the spread of illegal content, damaging malware and other criminal activities. By the time the authorities intervene, often there is no longer any trace of the criminals.

- **Anonymous Communications**: while total anonymity is difficult to achieve, technologies are built to protect individuals' privacy... with the effect also of assisting hiding the identity of those engaging in criminal activities.

- **Encryption Technologies**: this is becoming a target of national crime fighting authorities, as one of the most important steps in any criminal investigation is identifying the person who committed or participated in a criminal activity.

From a legal point of view, there are further difficulties in dealing with cyber-criminal activities:

- **Drafting criminal law**: the speed of technological development means that law-makers must continuously respond to internet developments and monitor the effectiveness of existing provisions. The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law.

- **New Offences**: often, crimes committed using ICTs are not new crimes, but illegal activities modified to be committed online. This can normally be dealt with is the drafting of existing criminal legislation is wide enough to cover the new technological means or circumstances. The situation is

different, if the acts performed are no longer addressed by existing laws, so it becomes necessary to adopt new laws criminalising computer-related fraud, in addition to the regular fraud.

- **Use of ICTs**. It is ever more important for law enforcement agencies and the judicial authorities to use ICTs within their functions for dealing with ICT related crime. New tools mean the need for more training and new investigative instruments (within the area of digital forensics).

- **Digital Evidence**: digital evidence – data stored or transmitted using ICTs that may show how an offence occurred – is now not just a "new source of evidence", but is becoming a principal source of evidence. Handling this digital evidence has unique difficulties (to preserve integrity and make it available in court) and requires specific procedures.

New developments such as cloud computing can have a significant effect on dealing with digital evidence. Enforcement agencies can no longer simply focus on the suspect's premises – today a lot of computing is done online with online tools and repositories for remote access. These may well be outside jurisdiction.

6.4. International dimension

One of the major challenges is that cybercrime often has an international dimension. Criminal law is usually national law, and other than war crimes there is little international legislation in this area. Cybercrime is the one area where in fact progress has been made to deal with international criminal activities, or simply local criminal activities that use international networks. In terms of illegal content, for example, internet users can access information from around the world, enabling them to access information available legally abroad, that could be illegal in their own country.

Within cybercrime investigations, a close cooperation between the countries involved is very important. This has been the focus of EU action, which cannot regulate crime but can provide a pan-EU system for police cooperation. However, a number of countries base their mutual legal assistance regime on the principle of "dual criminality" (international investigations are limited to those crimes that are criminalised in all participating countries). One of the key aims of international legal approaches is to prevent the creation of safe havens by providing and applying global standards.

At EU level, there have been several initiatives and legal documents:

- Eurojust.
- Communication on "Network and Information Security (2001). Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.
- Framework Decision on Attacks against Information Systems (NB this has been challenged and partially invalidated by the European Court of Justice for lack of legal basis).

- Data retention Directive: EU Directive on Privacy and Electronic Communication (see privacy module).

In 2008 the European Union started a discussion about a Draft Amendment of the Framework Decision on Combating Terrorism. The EU highlights that the existing legal framework criminalises aiding or abetting and inciting but does not criminalise the dissemination of terrorist expertise through the internet. With the amendment the European Union is aiming to take measures to close the gap and bring the legislation throughout the European Union closer to the Council of Europe Convention on the Prevention of Terrorism.

For a general overview, see the Justice, freedom and security area of the European Union and in particular the judicial cooperation in criminal matters.

Other international initiatives are:

- ITU Global Cybersecurity Agenda.

- Council of Europe:
  - *Convention on Cybercrime* that we have already mentioned and comment on below. In addition to the signatories, other countries such as Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have already drafted parts of their legislation in accordance with the Convention.

  - *First Additional Protocol to the Convention on Cybercrime*, covering racism and the distribution of xenophobic material (this was a controversial matter especially due to the conflicts with freedom of speech principles).

  - *Convention in on the protection of minors against sexual exploitation* (2007). Apart from the criminalisation of the sexual abuse of children the Convention contains a provision dealing with the exchange of child pornography and the solicitation of children for sexual purposes.

- OECD: OECD Guidelines for the Security of Information Systems and Networks., at

As a result of the difficulty of enforcing national criminal law in a context of international networks, national approaches tend to require additional measures (crimes) so as to be able to apply local law to these activities. One approach is to criminalise the provision or use of services (within jurisdiction) used in the committing a crime. This puts an additional burden on service providers, to police their own networks (see the debate on IPR enforcement and the HADOPI law in France, soon to be replicated to a certain extent in Spain and maybe the UK). This does not always work as most crimes are not strict liability but require an element of knowledge (*mens rea*) so that network service providers can avoid liability by arguing lack of knowledge. The EU

Ecommerce Directive bases ISP exemptions on this argument, and only engages their liability when they have effective knowledge of the activity or sufficient ancillary indications.

Hadopi Law – Loi favorisant la diffusion et la protection de la création sur Internet

In May 2009 France promulgated a law to control and regulate internet access as a means to encourage compliance with copyright laws. "HADOPI" is the government agency created by the law to monitor enforcement.

HADPOPI: *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* (High Authority of Diffusion of the Works and Protection of the Rights on Internet.

The general idea is "three strikes and out", meaning that after HADOPI has given a first warning to internet users if it suspects the user is carrying out illegal activities (i.e. subtext: file sharing), the ISP must monitor the internet connection. If the user does not stop, a second letter may be sent by HADOPI, the ISP or the rights holders. If the use still doesn't stop, the ISP is required to suspend the service for 2 months up to 1 year (and the user is blacklisted from getting services from other ISPs).

This raises serious questions regarding fundamental rights, including as to privacy (ISP monitoring the service), access to information (suspension of the internet connection), burden of proof and right to a judicial defence, etc.

Spain has a similar project underway (with a similar commission) and the UK, in April 2010, passed the controversial Digital Economy Act[2], including rights to block internet access, obligations on ISPs to notify users if the ISP itself is notified by IP rights holders that there "appears" to be an infringement.

[2]See it online at the OPSI (Office of Public Sector Information) site, comment at the Open Rights Group site and Wikipedia.

6.5. Substantive (cyber) criminal law

While this is not the place for a full treatise on cybercrimes, in this section we comment on some of the most important measures against cybercriminal activities, focussing on the Convention on Cybercrime (CoC).

- **Offences against the confidentiality, integrity and availability of computer data and systems:**
  - **Illegal Access (Hacking).** The CoC criminalises "unauthorised access to a system" thus protecting the integrity of the computer systems (Article 2 – Illegal access).
  - **Illegal Interception.** The CoC includes a provision protecting the integrity of non-public transmissions by criminalising their unauthorised interception (Article 3 – Illegal interception).
  - **Data Interference.** The CoC includes protects protection of the integrity of data against unauthorised interference. It provides computer data and computer programmes with protections similar to those enjoyed by tangible objects against the intentional infliction of damage (Article 4 – Data interference).
  - **System Interference**: To protect access of operators and users to ICTs, the CoC includes a provision criminalising the intentional hindering of lawful use of computer systems (Article 5 – System interference)

i.e. any act interfering with the proper functioning of the computer system.

- **Content-related offences:**
  - **Child Pornography**. The CoC includes an Article addressing child pornography to improve and harmonise the protection of children against sexual exploitation (Article 9 – Offences related to child pornography). This is reinforced by Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

- **IPR related offences:**
  - **Copyright infringements** (e.g. allegedly P2P file sharing, etc.) is a major concern of the content industry, which has significant presence and pressure in legislative circles. The CoC therefore includes provisions covering these copyright offences that seeks to harmonise the various regulations in the national laws (Article 10 – Offences related to infringements of copyright and related Rights). Unlike other legal frameworks the convention does not explicitly name the acts to be criminalised, but refers to a number of international agreements that already deal with this issue (WIPO Treaties, etc.).

- **Computer-related offences:**
  - **Computer related Fraud**. The CoC aims to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property (Article 8 – Computer-related fraud): "a. any input, alteration, deletion or suppression of computer data; b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

6.6. Procedural Law

As noted above, while achieving consensus on the definition and scope of various cybercrimes is one area, the other side of the coin is the introduction of procedures to enable enforcement agencies to take effective action against cyber-delinquency (in addition to training and equipment): procedural instruments that enable them to take the measures that are necessary to identify the offender and collect the evidence required for the criminal proceedings.

The main issue here is the digital nature of the evidence that is processed (collected, stored and produced), and the new media/means for transmitting it: the global ITC networks. This has led to the development of a new investiga-

tory "science", Computer Forensics (including computer and network Investigations) being specific data-related investigation techniques, including collection and analysis of relevant data.

Specific measures to facilitate the detection of cybercrimes include;

- Data retention obligations (obligation to preserve certain data at all times, e.g. traffic data) (Art. 16 CoC).
- Data preservation obligations (orders to preserve certain data once notified, not just limited to traffic data) (Art. 17 CoC).
- Data production obligations (orders to produce and disclose retained or preserved data) (Art. 18 CoC).
- Search and seizure orders (Art. 19 CoC).
- Real Time Collection of Data (Art. 20 CoC).
- Data interception (Art. 21 CoC).

On the other hand, care must be given to protect basic human rights and freedoms, ensuring that traditional safeguards are maintained in the digital environment. Criticism has been focused on the Convention on Cybercrime as it contains a number of provisions that establish investigation instruments but only one provision (Art. 15) that deals with safeguards, including some specific safeguards and a generic protection of "rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments..."

Another key topic and requirements for ICT related investigations is the international dimension: transnational investigations often require immediate reaction of counterparts in the country where the offender is located or data has either transited or been stored. The CoC provides a general framework for international cooperation, and in the EU this has been reinforced by instruments created by the European Commission under the Judicial Cooperation initiatives we mentioned above.

> Art. 23 CoC notes that the general principles do not only apply in investigations of cybercrimes, but in any investigation of any crimes where evidence in electronic form needs to be collected (e.g. if the suspect in a murder cases used an email service abroad).

Areas covered by this framework include;

- Extradition (art 26).
- Mutual help (art. 27): designated contact points for mutual legal assistance requests, direct communication between the contact points to avoid long lasting procedures and the creation of a database with all contact points.
- Mutual assistance regarding provisional measures (in relation to the measures set out above for criminal investigations: data retention, preservation, production, etc.).

- Transborder access to stored data.

Finally, it must be noted that significant pressure is being put on ISP (access and service providers) to cooperate and actively participate in the persecution and detection of cybercrime. While the operators themselves may benefit from exemptions of liability, these laws have also ensured and imposed obligations of collaboration with authorities and even carve-outs from exemptions when public or national security is involved.

6.7. Conclusions

Compared with private law (commercial, tort, etc.), criminal law in the ICT domain is less developed. However, most jurisdictions have implemented provisions, often deriving from the CoE Convention on Cybercrime, in their Criminal Codes or equivalent specific laws (like the UK Computer Misuse Act and others). So as regards substantive law, apart from the major areas of cultural differences there has been significant progress towards creating a harmonious international framework.

On the other hand, the Council of Europe has noted two significant problems:

- The process of implementation of the procedural law provisions, such as search and seizure, data retention – in particular regarding the conflicts with higher laws such as constitutional or international treaty safeguards of privacy.
- Obligations on ISPs and their involvement in detection and prevention.

Finally, we note that this area is one of a perpetual race between technologies used to perpetrate or hide crimes, and the same technologies used by authorities to detect (criminal forensics) and prosecute (cybercourts) crimes, on the one hand, and protect citizens and organisations on the other (cybersecurity).

Further reading

Sites:

- ITU: http://www.itu.int/ITU-D/cyb/cybersecurity/ and http://www.cybersecurity-gateway.org/legal_context.html
- Council of Europe:
- US Dept. of Justice: http://www.cybercrime.gov/

EU work:

- Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final: http://europa.eu/legislation_summaries/information_society/l33193b_en.htm

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems: http://europa.eu/legislation_summaries/information_society/l33193_en.htm

- Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005

on attacks against information systems http://eur-lex.europa.eu/LexUriServ/
LexUriServ.do?uri=CELEX:52008DC0448:EN:NOT

Other:

- http://www.cybertelecom.org/security/treaty.htm
- http://www.privacyinternational.org/
- http://en.wikipedia.org/wiki/Computer_crime
- http://www.crime-research.org/
- http://www.cybercrimelaw.org/
- http://www.cybercrime-institute.com/

Privacy

Index

1. Privacy – the protection of personal data

The processing of data that identifies people – or "personal data" – is necessary for the provision of the vast majority of information society services. Think of the parties to a contract or the names of passengers for an electronic ticket, the email address of users registered with web platforms, etc. What is often unnecessary is the extent of personal data processing carried out, in terms of the data gathered, the uses made of such data or data transfers to third parties.

Example

For example, many of us receive unsolicited emails or telephone calls, often as a result of the illicit use of our personal contact details (e.g. which have been provided to another telecommunications operator or to the same operator for another purpose, such a billing).

This has led to significant abuses and strict regulation within the EU on the use of personal data.

In this module we will consider the protection and control of the use of personal data within the European Union, both generally speaking and in the context of electronic services and communications.

First we introduce the concept of privacy and its legal framework (which establishes the obligations of companies and the rights of individuals), and then we will discuss how information society services can be affected by privacy obligations.

The legal texts currently in force within the European Union are:

- Council of Europe Convention 108 of 28th January 1981.
- European Directive 95/46, related to the protection of private individuals in terms of the processing of personal data and the free circulation of such data (the *Data Protection Directive* or *DPD*). The aim of the Data Protection Directive is to reconcile privacy protection with the free flow of trade. In particular, it sets out requirements for the legitimate processing of personal data and requires that specific care is given to sensitive data.
- European Directive (2002/58/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (*E-communications Directive*). The E-communications Directive provides specific rules for the processing of data related to provision of services over electronic communications networks (e.g. traffic and location data) and information security requirements in such networks.
- European Directive 2006/24/CE on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks (*Data Retention Directive*).

- National implementations of the privacy Directives, such as:
  - Spanish Organic Law 15/1999, on the Protection of Personal Data (the LOPD) and General Law on Telecommunications.
  - UK Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.
  - French "*Loi Informatique et Libertés*", 1978.

The Data Protection Directive came into force on 13 December 1995 and the deadline for implementation into each European Economic Area (EEA) Member State's national law was 24 October 1998. Member States interpret the Directive in slightly different ways, so when considering data protection issues, attention should be given to the national data protection legislation passed in the country concerned (as well as the Data Protection Directives).

Supplementary content
For EU legislative and case law references, see the European Commission site.

2. Basic concepts

Privacy protection regulations are designed to guarantee and protect personal data, public freedoms and the fundamental rights of private individuals, especially their right to personal and family honour and privacy.

There are requirements relating to the quality of the data and the legitimacy of the data processing. The Data Protection Directive also provides for extensive individual rights, not least the rights of access and rectification, and restricts trans-border data flows outside the EEA to those states without adequate protection. It also significantly strengthens security requirements for processing.

There are a number of specific exemptions and restrictions set out in the Data Protection Directive. These are not dealt with in any detail in this report. Suffice it to say that the scope of the principles relating to the quality of the data, information to be provided to the data subject, right of access and the publicising of processing may be restricted in certain circumstances. Such circumstances include the interests of national security, public security, the prosecution of criminal offences, important economic or financial interests of a Member State or the EU or the protection of the data subject.

2.1. Key definitions

In order to understand the legal framework of privacy, it is important to consider the following basic concepts:

- **Personal data**: any information relating to an identified or identifiable natural person ("data subject"). There is a sub-category of data that is especially protected (ideology, religion and beliefs, racial origin, health, etc.).
- **Files/filing system**: Any organised set of personal data, irrespective of its form or modality of creation, storage, organisation and access. This can extend to non-automated files (on paper) and to any type of personal data prone to handling.
- **Processing**: 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.
- **Data Subject**: The private individual owner of the data that is subject to processing.
- **Data Controller**: 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 (what, who, how, when

and where). The data controller is liable administratively, civil and poten-
tially criminally, for potential infringements of privacy laws.

- **Data Processor**: The person who, either alone or in conjunction with oth-
  ers, processes data on behalf of the data controller. A common example is
  where an organisation appoints a third party IT company to provide data
  processing services to that organisation on an outsourcing basis.
- **Data Protection Agency**: a national authority with power to sanction is
  set up in order to guarantee the protection of personal data and to keep
  notified file registers (e.g. the Spanish *Agencia Española de Protección de
  Datos* or the *Information Commissioner* in the UK, *CNIL* in France).

As examples of files containing personal data, one could cite any set of data
such as the medical histories of a doctor's patients (on condition that they are
arranged following logical criteria) or the profile of users of a website (clients,
registered individuals, etc.). It doesn't matter whether the data "format" is
physical or electronic, nor is it relevant (in principle) whether it is subject or
not to automated processing.

2.2. Roles

As we can see from the definitions, one of the key decisions in analysing data
protection responsibilities is determining the status of the parties involved. In
particular, this involves deciding which parties are data <u>controllers</u> and which
parties are mere data <u>processors</u>. The *data subject* is the person whose data is
being processed.

Data Controllers have the responsibility for ensuring compliance with data pro-
tection legislation, both at a national level and with the Data Protection Di-
rective. Determining the status of the parties is not always so clear cut. In some
circumstances, for example in joint ventures where there may be a number of
organisations purporting to operate as a single entity, it may be more suitable
for those organisations to act as joint controllers of the personal data.

Data Processors process data on behalf of the Data Controllers, and are subject
to certain obligations, particularly as to security.

The E-communications Directive introduces two additional roles: the *public
electronic communications network provider* and the *public electronic communica-
tions service provider*. These actors are responsible for the processing of traffic
and location data, which will be explained in further detail below.

- The *public electronic communications network provider* operates the pub-
  lic electronic communications network (defined in Telecommunications
  Framework Directive) to include the operators of the relevant network in-
  frastructure regardless of the technology used, made available wholly or
  mainly for provision of electronic communications services to the public
  (e.g. not enterprise networks and other internal systems).

- The *public electronic communications service provider* offers electronic communications services to the public, being generally speaking the "conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting". This excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services and information society services that we have commented on before.

These roles include traditional telecommunications operators who provide both the networks and the services on the network (fixed line and wireless voice and data carriers, e.g. telephone companies and internet access providers).

In relation to these services, the E-communications Directive introduces the concepts of "subscriber" referring to the person or entity which subscribes to electronic communications services, and "users", being the end-users of such services. The users may be data subjects under the Data Protection Directive.

2.3. Data processing

Privacy laws generally apply to the processing of personal data by automatic means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (i.e. traditional paper files) and to any form of subsequent use of such data by the public and private sectors.

In some jurisdictions, certain categories of personal data are excluded from protection:

- Files held by private individuals in the course of their exclusively private or domestic activities (for example a personal agenda).
- Professional contact details, on condition that they refer to the company where the interested party works (name and surname, telephone, fax number, business address and electronic mail).
- Files related to national defence and the protection of the State, terrorism and serious forms of organised crime.

2.4. Territorial application

The general rule is that a data controller who is established in an EEA state must abide by the national law applicable to the place in which it is established. If the data controller has establishments in more than one EEA state he must follow the relevant national law for each establishment. Those laws will also apply to data controllers outside the EEA when processing is carried

out using equipment within the territory. This gives rise to certain questions with respect to online processing of personal data by a controller established outside the EEA.

> Thus the Spanish "LOPD" will apply to processing carried out on Spanish territory in the context of the activities of an establishment belonging to the data processor in Spain or in the European Union, or when the data processor is not established on Spanish territory but Spanish legislation applies in accordance with Public International Law. Regulatory security obligations apply to third party data processors on Spanish territory.

3. General principles

The Privacy laws establish certain general principles that must be observed with regard to the processing of personal data.

Generally speaking, as explained above, in order to process personal data lawfully, the data controller must identify a ground which justifies the processing. The criteria for lawful processing depend on the kind of data that is processed, i.e. general personal data, sensitive data, communications traffic or location data. These criteria aim at a somewhat broader principle of minimalism, i.e. that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are collected and further processed. This principle is also reflected in the strict rules on processing location and traffic data.

- **Data quality**. Article 6 of the Data Protection Directive sets out the three data quality requirements which shall be determined according to the specific case in question. These state that personal data must be:
  (a) Adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed (Article 6(c));
  (b) Accurate and, where necessary, kept up to date (Article 6(d)); and
  (c) Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were collected or for which they are further processed (Article 6(e)).

- **Purpose**. In addition, there is a purpose requirement. Article 6(b) states that "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Personal data may not be used for purposes that are incompatible with the reason for which it has been gathered and when the designated purpose has been fulfilled, it must be cancelled or destroyed.

  "Yahoo! uses information for the following general purposes: to personalise the advertising and content you see, based on the details given by you at registration and your activity at Yahoo!, fulfil your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients. You agree that Yahoo! may transfer your personal information for the general purposes set out above to any Yahoo! group company worldwide." Yahoo.co.uk Privacy policy, March 2010.

- **Information** (Art 10). Data subjects must be informed beforehand expressly, clearly and unequivocally of (a) the identity of the controller and of his representative, if any, (b) the purposes of processing for which the data are intended; and (c) any other information necessary to guarantee fair processing, having regard to the circumstances. In practice, information should be provided as to whether or not it is compulsory to provide the data, and how to exercise rights of access, rectification, cancellation

and opposition. If this information is not provided when the data is collected, then it must be provided later when processing is carried out (e.g. where the data have not been collected directly from the data subject).

In practice, the information is generally provided in the form of a data protection notice, which can be given to the data subject via application forms, terms and conditions, by telephone or on a website. By using an appropriately worded data protection notice, an online business can ensure that there is consent from visitors to its website to allow the business to build a valuable contacts database and market the visitors.

- **Data subject consent** (Art 7): The processing of personal data will require the informed, unequivocal, express or tacit, consent of the data subject, given freely (i.e. within the possibility to refuse), unless the law states otherwise (in other words, a legal authorisation, e.g. by court order). The processing of data that is especially protected requires express consent in writing. Certain categories of data or processing do not require consent, for example, data gathered from sources accessible to the public, data in commercial or employment contracts, or when processing is "necessary" to comply with a legal requirement, to protect the vital interests of the data subject (e.g. medical data) or for the *legitimate interests* pursued by the controller.

This last ground is particularly useful to avoid the requirement for express consent, however some European jurisdictions (e.g. Spain) have not implemented this part of the Data Protection Directive, for constitutional reasons, which greatly limits the processing purposes that can be legitimised there. Relying on this ground is subject to challenge by a data subject who can show that processing is nevertheless prejudicial to his rights or freedoms or legitimate interests.

- **Confidentiality**: Both the data controller, and the data processor, as well as any other party intervening in any phase of the data processing, are obliged to professional secrecy in relation to the data and to maintain secrecy.

- **Data communications**: Subject to several exceptions, any communication or transfer of data to a third party requires the prior authorisation of the interested party.

In addition, the laws establish that it is generally forbidden to process "sensitive" personal data, i.e. that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and information concerning health or sex life, unless consent has been granted or in other specified circumstances.

4. Rights and obligations

As a result of these principles and other dispositions of the laws, the data subject benefits from various rights and the data processor is subject to a series of obligations.

4.1. Data subject rights

Data subjects have the following rights:

• To receive the abovementioned information at the time that the data is gathered (see above).

• To access, rectify and cancel such data, with a view to maintaining the accuracy of the data, rectifying or cancelling it when it is incomplete or inexact, inadequate or excessive for the purpose.

> The right to access is one of the most important rights available to data subjects under the Data Protection Directive. An individual may request access to all personal data of which he or she is the subject and which is being processed by the controller. In some jurisdictions, the controller may require the data subject to pay a maximum fee, (in the UK it is £10, however in Norway there is no fee imposed), to make the request in writing and to provide enough information to identify and verify the identity of the data subject making the request.

• To object and oppose processing of his/her data, when there are legitimate justified grounds relating to a specific personal situation and in particular to processing of personal data which the controller anticipates being processed for the purposes of direct marketing (and must be informed and given the right to object if data is disclosed to third parties for these same purposes).

• To contest any administrative or private action that involves an assessment of one's behaviour on the basis of the automated processing of one's personal data.

Example

An example of an automated decision is where a financial services company uses an automated system to target, select and, more importantly, reject customers for particularly good credit offers.

• In addition, where there is a general register of data files (Data Protection Agencies), the data subject is usually granted the right to consult the register free of charge.

Every person has the right to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

4.2. Data controller and processor obligations

The data controller is subject to various obligations, the main ones being:

- To observe the general principles of data protection.
- To notify and register the data files with the Data Protection Agencies before carrying out any processing (Member States may dispense with this in certain circumstances). The Data Protection Directive (DPD) sets out certain information that must be notified, including the name and address of the controller, the purpose of processing, categories of data subject, categories of data, recipients of the data, details of transfers abroad and details of any security measures to be taken.
- To provide the interested party with the information mentioned above and to obtain their consent when necessary.
- To guarantee the procedures that allow data subjects to exercise their rights of access, rectification and cancellation.
- To document relationships with third parties intervening in the processing and, in particular, to ensure data processors only access data pursuant to a contract (see below).
- To implement the security measures of a technical and organisational nature necessary to guarantee the safety of the data under processing (see below).

A data processor must also fulfil the obligations included in the data processing contract: to carry out the activity on behalf of the data controller and to process the data in accordance with the instructions received. In the event of breach the obligations applicable under the privacy laws, the data processor will respond personally for any breaches committed.

5. Access to data and data transfers

5.1. Access by data processors

"Access to data" is understood to mean when a third party accesses the data in order to provide a service to the data controller. This third party is referred to as the "data processor". Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller.

Data processors

There are many examples of "data processors". Basically, it refers to the majority of information technology service providers that access or can access their clients' data:

- Data processing centres (outsourced).
- IT service providers (IT support, helpdesks, etc.).
- Customer care centres (which access user data).
- Companies providing web services, hosting and even data or email processing services (Amazon Web Services, Google Apps).
- Paper disposal companies.

The relationship must be governed by contract (often called an "Art 17 contract", under Article 17 of the DPD), which must be in writing and set out what the processor may or may not do with the personal data, including what security measures should be taken to safeguard the data. In particular, the data processor must implement the security measures indicated by the data controller.

> **Supplementary content**
>
> Controllers should reserve for themselves the right to audit processors to ensure compliance with the contract.

5.2. Data Transfers

Data transfers are not defined in the Directive, however Member States have generally provided that a transfer of data is any communication of personal data to a person other than the interested party, as distinct from an "access" to data as we have discussed above.

Data transfers

Typically, there is a transfer when data is transferred between a subsidiary and a parent company, from an HR consulting firm to its clients, from a doctor to a hospital or medical insurance company, or when marketing databases are sold (list of email addresses, etc.).

Personal data may only be transferred for the fulfilment of purposes directly related to the legitimate functions of the assignor and assignee and, with several exceptions (legal authorisation, etc.), must always have the prior informed consent of the interested party.

5.3. International data transfers (outside the EEA)

The concept of international data transfer covers both access to data by a data processor as well as its communication to third parties outside the EEA (EU Member States together with Iceland, Liechtenstein and Norway). Note that the mere transit of data via internet servers outside the EEA (email, web pages) does not count as a data transfer.

> Following the ECJ decision in the Swedish case against Lindqvist (C-101/01) in November 2003, data is not "transferred" to a third country where an individual in a Member State merely loads personal information onto a website that is hosted in that State or another Member State, so that the information can be accessed by anyone who connects to the internet.

As a general rule, the international transfer of data is only allowed when the destination is a country that ensures an "adequate level of privacy protection", i.e. offering the same level of protection as that provided by the DPD (article 25 DPD). This includes by default the EEA members, and also any other country approved by the European Commission (or an applicable Data Protection Agency) due to providing an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

> The countries approved to date are: Argentina, Canada, Hungary, Switzerland and the UK Island of Guernsey (and the US under the principles of "Safe-Harbour" and the transfer of Air Passenger Name Records to the United States' Bureau of Customs and Border Protection).

International transfer is also allowed in some other specific cases, for example, when (a) the recipient has signed a contract guaranteeing similar levels of data protection or (b) transfers between members of a business group that establishes a suitable internal policy for the protection of privacy (Binding Corporate Rules).

The availability of contractual safeguards is important, enabling data processors or controllers in third party countries to sign contracts with data controllers in the EEA (on the basis of the approved model clauses provided by the Commission) for the processing of data outside the EEA.

> Decisions 2001/497/EC and 2002/16/EC (now Commission Decision of 5 February 2010, C(2010) 593) set out standard contractual clauses for the transfer of personal data to third countries (data controller to data controller and data processor, respectively). A further Decision was passed in 2004 which introduced an alternative set of standard contractual clauses for the transfer of personal data to third countries.

Article 26 of the Data Protection Directive sets out a number of derogations (i.e. exceptions) to the aforementioned prohibition, so that transfers to third countries may be permitted where:

(a) The data subject has given his consent unambiguously to the transfer;
(b) The transfer is necessary for the performance of a contract between the data subject and the controller;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

(d) The transfer is necessary or legally required on important public interest grounds or for the defence of legal claims;

(e) The transfer is necessary to protect the vital interests of the data subject; or

(f) The transfer is made from a public register.

The most commonly used of these derogations is (a) consent. Consent must be specific and informed. This means the individual must know and understand what such consent will amount to. Data subjects should be informed of the reasons for the transfer and the countries involved. In the data protection notice, controllers will often draft the notice widely and in particular will state that transfers to third countries may take place as a way of extracting consent from the data subject to such processing.

6. Security obligations

The data controller and, where applicable, the data processor, are obliged to implement appropriate (security) measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Google Privacy Policy, March 2010

"Information security. We take appropriate security measures to protect against unauthorised access to or unauthorised alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorised access to systems where we store personal data."

The Data Protection Directive does not predicate any particular measure and the member states of the European Union have taken different approaches to the issue, from self-regulation (UK) to detailed compulsory measures (Spain).

Under the Spanish Data Protection Laws, three levels of protection are established according to the type of information handled. The basic level applies by default to any personal data file, whereas the medium level applies to files containing data related to administrative or criminal violations, the Tax Authority, financial services, and credit ratings; and the high level applies to files containing data regarding the ideology, religion, beliefs, racial origin, health or sex life and data gathered for police purposes without the affected party's consent.

The different levels of safety involve obligations that are increasingly burdensome for implementation by the data controller and any processor (Security Manager). The basic obligations include preparing a security document and a register of incidents as well as defining the functions of the people with access to the data. Plus, for medium and high levels, a periodic (technical-legal) audit of the security measures implemented for the high level must take place, carrying out backup copies and encoding data transmissions.

7. Regulatory supervision

The DPD provides that the national Data Protection Agencies (supervisory authorities) must have certain powers to regulate the processing of personal data. This includes:

- Investigative powers, such as access to data processing operations and the collection of all the information necessary for the performance of its supervisory duties.
- Powers of intervention (delivering opinions before processing operations are carried out, ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, of warning or admonishing the controller).
- The power to engage in legal proceedings where the data protection provisions have been violated.

National laws have provided these powers, and included powers to fine data controllers and processors for breach of the privacy obligations.

Spain

In Spain, the LOPD systematises the potential violations of the Law, classifying violations related to the protection of personal data. While there is no exhaustive list, the Agency can sanction any breach of the data subjects' rights (informed consent, rights of access, rectification and cancellation), lack of collaboration on the part of the Agency, lack of compulsory notifications or the creation, processing, communication, transfer and maintenance of files without observing the terms of the law. Breaches can entail fines between 600 and 600,000 Euros (per breach).

Various sanctions have been published, despite their alleged secrecy:

- In 2000,) a TV company Zeppelín was fined 1.1 million Euros for disclosing data on candidates for the Big Brother programme (this has been appealed).
- In 2001, Telefónica de España and Telefónica Data were fined 841,420 Euros for exchanging their client data.
- In 2002, the company Inlander had to pay 300,000 Euros for having its server installed in the United States.
- In 2008, the collecting society "SGAE" was fined 60,101 Euros for recording a wedding (to collect evidence of non-payment of levies).
- In 2010, Citybank España was fined 60,101 Euros for sending communications without consent (to one person!).

8. The legal framework for data privacy in other jurisdictions

Outside of Europe, we observe that due to the effect of these obligations and, especially, those relating to the international transfer of data, most commercial partners of European countries are almost "obliged" to establish similar legal frameworks for the protection of privacy. We would mention Canada, Switzerland and Argentina, which have been approved by the European Commission, but also Japan or Australia.

The United States is a special case, which has much less privacy protection than Europe, and which is organised by sectors: especially, for banks and financial services and the health sector. In order to allow the transfer of data from the EU, the US has established a quasi-private regime, by means of the Safe Harbor agreement of July 2000.

Safe Harbor

The decision by US-based organisations to comply with the Safe Harbor Privacy Principles is entirely voluntary. Organisations need to self-certify annually to the US Department of Commerce and state in their published privacy statement that they adhere to the principles. The Safe Harbor Principles impose obligations with respect to security and the appointment of data processors that are generally equivalent to those set out in the Data Protection Directive. US organisations can also meet the adequacy requirements of the Data Protection Directive if they include the Safe Harbor requirements as the substantive privacy provisions in written agreements with parties transferring data from the EU.

To date, approximately 2,000 US companies have signed the agreement. Others have signed standard contracts undertaking to protect the data appropriately.

9. Privacy in the sector of electronic communications

New technologies, in particular internet and email, must fulfil certain require-
ments in order to guarantee the right to privacy. The amount and intensity
of communications as well as the nature of data transmitted can be a risk
for people's privacy. Therefore, to improve people's confidence in the use of
telecommunications, a series of rules have been established imposed on elec-
tronic network and service providers. These were established by the E-com-
munications Directive and the Data Retention Directive.

9.1. Telecommunications secrecy

Member States within the EU generally impose obligations of confidentiality
and secrecy in respect of telecommunications.

The three basic principles are:

- **The secrecy of communications**: the confidentiality of communications
  carried out through public electronic communication networks must be
  guaranteed. In particular, it is prohibited for people other than users to
  listen to, intercept or store communications without the prior consent of
  users or a court order.
- **Interception**. The laws develop the principles for the interception of elec-
  tronic communications by agents of the public administrations. Data pro-
  tection confidentiality obligations are only restricted in order to carry out
  investigations into criminal activities or to guarantee national security,
  public defence and safety, in conditions where the lifting of confidential-
  ity constitutes a "necessary, proportionate, and appropriate measure in a
  democratic society".
- **Encryption**. The encryption of data circulating on electronic communi-
  cation network is normally allowed (e.g. Skype encrypts messaging), how-
  ever certain national laws also allow the authorities to demand handover
  of the encryption keys.

The E-communications Directive reiterates these basic principles, providing
that Member States must ensure the confidentiality of communications made
over a public electronic communications network. They must, in particular,
prohibit listening, tapping and storage of communications by persons other
than users without the consent of the users concerned.

9.2. Electronic communications

9.2.1. Traffic data and Location data

The E-communications Directive defines:

- **Traffic data** as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". The definition covers data such as call data, addressing or numbering data (e.g. IP-addresses or phone numbers), data relating to the routing, duration, time, protocol used, or data generated for the purpose of billing.

- **Location data** as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

- Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Processing of traffic data may only take place to the extent and duration necessary to fulfil certain specified purposes: subscriber billing and interconnection payments, marketing electronic communications services or providing value added services provided the user or subscriber has given prior consent; or fraud detection, traffic management and handling customer enquiries.

  Service providers must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing. This information must be provided before obtaining consent to marketing electronic communications services or providing value added services. Users or subscribers shall also be given the possibility to withdraw their consent for the processing of traffic data for these purposes at any time.

  The Directive also sets restrictions on the entities that are allowed to process traffic data. Traffic data may only be processed by persons acting "under the authority" of electronic communications network or service providers (i.e. internet access providers, mobile operators, etc.).

  This requirement suggests that the persons involved in the processing of traffic data either have to be employed by the network or services provider, or that third parties must be appointed as a processor in accordance with the Data Protection Directive.

- Location data (other than traffic data) can only be processed if it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision of any services. The service provider must inform the users or subscribers, prior to obtaining their consent of: the type of location data which will be processed; the purposes and duration of the processing; and whether the data will be transmitted to a third party for the purpose of providing the value added service.

  Users or subscribers must be given the possibility to withdraw their consent for the processing of location data at any time and also, using a simple means and free of charge,

to refuse temporarily the processing of such data for each connection to the network or for each transmission of a communication.

Restrictions similar to those applicable to traffic data are imposed on the entities and persons that can process location data (e.g. persons involved in the processing of location data either have to be employed by the network or services provider, or that third parties must be appointed as a processor in accordance with the Data Protection Directive).

9.2.2. Security requirements

The E-communications Directive sets out additional security measures in relation to the processing of personal data in the electronic communications sector. The provisions of the Data Protection Directive are reinforced, as providers of publicly available electronic communications networks must take appropriate technical and organisational measures to safeguard the security of its services.

The E-communications Directive also regulates the use of cookies (hidden information exchanged between an internet user and a web server that is stored in a file on the user's hard disk, which is useful for monitoring a net surfer's activity). Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. To that end, notice of uses of cookies must be given and users must be able to decide not to accept cookies, except where the cookie is essential to deliver contracted services.

UK Information Commissioner website

"We use Google Analytics to help analyse use of our website. This analytical tool uses 'cookies', which are text files placed on your computer, to collect standard internet log information and visitor behaviour information in an anonymous form. The information generated by the cookie about your use of the website (including your IP address) is transmitted to Google. This information is then used to evaluate visitors' use of the website and to compile statistical reports on website activity for the ICO. To find out more about cookies, including how to control and delete them, visit www.aboutcookies.org/".

9.3. Data Retention

In March 2006, Directive 2006/24/CE was adopted regarding the preservation of data generated or processed in relation to the provision of services of electronic communication of public access or of public communication networks. The purpose of the Directive was to harmonise the rulings of Member States regarding the obligations of electronic communication service providers related to data preservation.

This Directive establishes the obligation to preserve certain categories of data by electronic communications service providers. The aim is to guarantee that such data is available for purposes of investigating, detecting and judging violations.

The Directive defines:

- The categories of data that need to be preserved: e.g.
    - Data regarding travel and location of private individuals and legal entities.
    - The data listed as necessary for identifying a subscriber or registered user.

- The periods for the preservation of data (basically, 12 months).
- The storage requirements for preserved data (guaranteeing confidentiality).
- The regime for transferring the data to public authorities, following a court order.
- The principles that must be respected in terms of data security, in accordance with the DPD.

Supplementary content

The scope of application of the Directive excludes the content of electronic communications; including information consulted using an electronic communication network.

10. Conclusions: the impact of privacy on technological projects

One cannot underestimate the impact of data protection regulations on technological projects. The obligations to inform and obtain the consent of the user and regarding data security are very cumbersome when there are millions of users involved. The prohibition of international data transfers determines where data processing, outsourcing or customer care services can be located, (for example, in Argentina or Canada, countries approved by the European Commission).

The viability of certain projects has been questioned due to the cost of fulfilling privacy obligations and restrictions regarding the use of personal data.

It is fundamental to carry out an impact study of the privacy obligations on the project's systems, processes and costs during the project's analysis, as well as to determine who is responsible for implementing the corresponding obligations (data gathering with prior information to the user, etc.) and notifying files to the Data Protection Agencies.

Very briefly, this analysis implies:

- Determining the category of personal data processed by the project's systems.
- Identifying who is responsible for these data (the person who determines the purposes of processing, the "owner" of the data).
- Establishing the obligations to inform, obtain consent and prove it (acceptance registers, etc.) and how they are implemented (web privacy policies, client documentation, etc.).
- Establishing the levels of security to be implemented, their implementation and corresponding cost.
- Defining the processes to respond to access and cancelation requests by interested parties.
- Identifying third parties with access to the data (data processors – data hosting companies, outsourcing companies, software and technology maintenance services, etc.) and, where applicable, the transfers of data to third parties, which must be justified.

Open standards

Index

1. Concepts

1.1. Open standards

A standard is generally a norm or specification regarding engineering or technical criteria, methods, processes and practices, generally achieved through a consensus of interested parties. Standards are usually created within the auspices of formal organisations like ITU, ISO, IETF, W3C, OASIS, etc.

Examples of standards in the technology arena

- **HTML** (HyperText Markup Language): specification of markup language for web pages.
- **XML** (Extensible Markup Language): a set of rules for encoding documents electronically.
- **SOAP** (Simple Object Access Protocol): a protocol specification for exchanging information in the implementation of web services.
- **Unicode**: a standard for the consistent representation and manipulation of text expressed in most text editing systems.
- **ODF** (Open Document Format): an XML-based file format for representing electronic documents such as spreadsheets, charts, presentations and word processing documents.

While there is no definition of an **open** standard –this is one of the key elements of the debate about open standards– it is generally considered to be a standard created through a process where any interested party may freely participate and collaborate (with formalised open standards organisations or committees or not) and made available to the general public on a royalty free and non-discriminatory basis.

It has been argued that an open standard is more than a mere specification. An open standard is "open" because of the principles behind it and because of the way in which it has been publicly developed, approved and made accessible. It is governed by a collaborative and consensus driven process.

An open standard is generally built on the principle that it is available for every end-user to obtain, read and implement, with no royalty or fee. Certain parties have argued that a fee may be imposed (e.g. for certification of compliance by a standards organisation), which must then be a low or reasonable cost (RAND). However, for many that is not acceptable (see below).

An open standard is also based on the principle of non-discrimination, so that no software producer is favoured over another other with respect to an implementation of the standard, other than through the producer's own technical

Author citation

"An open standard is more than just a specification. The principles behind the standard, and the practice of offering and operating the standard, are what make the standard Open."
Source: Bruce Perens

skills and efficacy. Consequently, copyright or patents which cover standards – one way of achieving discrimination – must be licensed royalty-free and without discriminatory terms, if the standard is to be "open".

The principles of open standards further include the possibility for obtaining an extension or subset form of the implementations.

All this is developed further below.

1.2. Definitions?

One of the current difficulties in relation to "open standards" is that there is no universal definition. In fact, there are different definitions for both terms "Open" and "Standard" and there are different levels of application of standards at national, regional, international levels with "internationally recognised standards" bodies playing a big role in this area.

Some internationally recognised standards organisations refer specifically to "open standards" whilst others refer simply to producing "standards". For instance,

- IEFT (Internet Engineering Task Force) and ITU-T (the standards developing organisation in the Telecommunication Standardisation Sector which coordinates standards for telecommunications on behalf of the International Telecommunication Union) refer to *open standards*.

- IEC (International Electrotechnical Commission that prepares international standards for all electrical, electronic and related technologies) and the ISO (the International Standard Settling Body) only refer to producing "standards".

Hence the term "open standard" on its own is not a term which has a universal understanding. Its definition often depends on geographic region, on the particular standards body or organisation and on the context and field of use.

What generally appears to remain universal in all the various definitions are the common principles of:

- Public participation in creation.
- Public availability.
- No royalty.
- Non-discrimination.
- The possibility of obtaining an extension or subset form to the implementation.

Supplementary content
In fact the IETF does not have its own specific definition of "open standard". However, the IETF standards fulfil (and may therefore be considered to share) the ITU-T's definition of "open standards".

In other words, an open standard must be accessible to anyone and there should be no restrictions to implementation and or discrimination between users. It is usually free of charge and not subject to any payment of any intellectual property rights or legal rights necessary to use, deploy or distribute their implementation.

> The term "open standard" is also sometimes coupled with "open source" with the idea that a standard is not truly open if it does not have a complete free/open source reference implementation available (c/f Tim Simcoe: Chapter 8; open standards and Intellectual Property Rights', to appear in Open Innovation: Researching a New Paradigm). See below.

Thus there are a number of approaches, some of which are commented below.

1.2.1. ITU-T definition

Within the ITU, "open standards" are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. "Open standards" facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

Other elements of "open standards" include, but are not limited to:

- Collaborative process – voluntary and market driven development (or approval) following a transparent consensus driven process that is reasonably open to all interested parties.
- Reasonably balanced – ensures that the process is not dominated by any one interest group.
- Due process – includes consideration of and response to comments by interested parties.
- Intellectual property rights (IPRs) – IPRs essential to implement the standard to be licensed to all applicants on a worldwide, non-discriminatory basis, either (1) for free and under other reasonable terms and conditions or (2) on reasonable terms and conditions (which may include monetary compensation). Negotiations are left to the parties concerned and are performed outside the Standards Development Organisation (SDO).
- Quality and level of detail – sufficient to permit the development of a variety of competing implementations of interoperable products or services. Standardised interfaces are not hidden, or controlled other than by the SDO promulgating the standard.
- Publicly available – easily available for implementation and use, at a reasonable price. Publication of the text of a standard by others is permitted only with the prior approval of the SDO.
- On-going support – maintained and supported over a long period of time.

1.2.2. European Union definition

The European Union on the other hand adopted the following definition in its European Interoperability Framework: (c/f European Interoperability Framework for pan-European eGovernment Services, Version 1.0 (2004) ISBN 92-894-8389-X page 9).

The minimal characteristics of an open standard are:

- The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision, etc.).
- The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee.
- The intellectual property – i.e. patents possibly present – of (parts of) the standard is made irrevocably available on a royalty-free basis.
- There are no constraints on the re-use of the standard.

1.2.3. Spanish law definition

In Spain, a law passed by the Spanish Parliament (c/f Ley 11/2007[1] of Electronic Access of Citizens to Public Services, June 22, 2007), requires that all electronic services provided by the Spanish public administration must be based on (1) open standards or (2) "eventually, on an ancillary basis, standards that are generally used by citizens" (which is not very satisfactory from a "open standards" perspective, and raised considerable debate).

It defines an open standard as royalty free, according to the following definition:

An open standard fulfils the following conditions:

[1]See Annex to the Law 11/2007 online at noticias juridicas site.

- It is public, and its use is available on a free [gratis] basis, or at a cost that does not imply a difficulty for the user.
- Its use is not subject to the payment of any intellectual [copyright] or industrial [patents and trademarks] property right.

1.2.4. Open Source Initiative's Requirement

The Open Source Initiative (OSI) is an organisation that promotes open source software (OSS) (see Module 4). As to the Open Standards Requirement (OSR) for open source software (OSS), the Open Source Initiative defines its requirements and criteria as follows:

- All necessary detail and any process for fixing flaws discovered under implementation and interoperability testing must be disclosed for interoperable implementation under terms which comply with OSR. In other words, no relevant detail must be withheld.
- The open standard must be freely available and accessible under royalty fee terms at reasonable and non-discriminatory cost.
- All patents essential to implementation of the standard must be licensed under royalty fee terms for unrestricted use or be obliged to a pledge of "non-assertion" in relation to open source software.
- There must be no agreements to execute a licence agreement, Non Disclosure Agreement, grant, click-through, or any other form of paperwork to deploy conforming implementations of the standard.
- Implementation of the standard must also not require any other technology that fails to meet the criteria of this requirement.

The above criteria must be met otherwise it will discriminate against open source developers.

2. Standardisation processes – forums

There are generally three levels of standards according to where they are created:

- National standard via national standards organisations.
- Regional standard via regional standards organisations.
- International standard for example international standards organisations such as IETF, IEC, ITU-T and ISO (ISO in itself is composed of various national standards organisations.).

Standards bodies are however only a method of achieving standardisation. There are also other types of standards for example industry de facto and government standards.

- **Industry de facto standards** are popular because the benefits of standardisation are often very high, increasing the user's ability to interoperate with others. The downside is that proprietary technology is often required which necessitates the payment of licensing fees to the relevant providers of that technology.
- **Government standards** on the other hand, can be provided via enforceable laws or regulatory body mandates adopting such government standards.

The main distinction between industry de facto / government standards and open standards is the element of openness in the collaborative efforts to create the standards, specifications and technology. Such openness and collaborative efforts are meant for easy accessibility and widespread use in order to implement those specifications.

3. Benefits of open standards

Why is there a need for open standards?

Author citation

As the Free Software Foundation Europe (FSFE) states: "open standards allow people to share all kinds of data freely and with perfect fidelity. They prevent lock-in and other artificial barriers to interoperability, and promote choice between vendors and technology solutions."

By adopting an open standard, the end-user/customer is not locked into a particular vendor. This decreases reliance of any one vendor specification, thereby maximising end-user choice resulting in a more competitive market for implementation of the standard. This ever more important in a networked world where more and more data and applications move to the net (in "computing clouds") and users lose direct control of their data and need interoperability to maintain a degree of control and be able to "exit" the cloud if necessary.

Supplementary content

Think of the HTML standard. Due to this standard, Netscape Navigator and subsequently Firefox web browsers managed not only to exist and survive, but also ensure compliance with the standard by web page developers and other browsers.

Generally speaking, open standards can achieve the following:

- They promote interoperability and integration between various applications or networks.
- They can consolidate competing standards and overcome differences in technical regulations and to decrease barriers in commerce (from local to international).
- They can facilitate not just application integration but also data exchange or integration among different products, components or services; and decrease duplication which enable applications to work together to perform or complete a process.
- They enable an increased representation of diverse interests and stakeholders in building the ICT infrastructure of our networked society. This leads to continual improvements, wider support, increased vendor competitiveness and flexibility.
- They reduce risk for end users who use solutions that comply with open standard specifications, being able to swap applications in the event of any disaster or unforeseen circumstance, and enable them to integrate their systems with third parties such as government, suppliers, customers and partners.

Let us look at two examples

- **Interoperability**. The use of the internet's TCP/IP communications protocol created a worldwide infrastructure for collaborating and coordinating resources since virtually any component on a network can communicate with any other component. The use of the TCP/IP open standard by any stakeholder allows them to use the specifications to build their own solutions. As interoperability increases and barriers to integration of disparate system decreases, one's ability to automate processes between technologies, platforms, languages and customisations increases correspondingly.

- **Integration**. As the standards of web services (SOAP, etc.) whose protocols are based on open standards achieve and gain growing acceptance, it is clear that originally economically infeasible web platforms can now be created through integration of different components. The "plug and play" concept to integrate devices and computer component is an example of such integration. It is simply based on a standardisation of integration specifications with an automation of common requirements.

An open standard, by helping to define component interfaces, increases interoperability. This leads to simpler, repeatable and quicker integration efforts. Besides, the use of an open standard effectively replaces many unique vendor solutions and increases the availability of resources sharing the same processes. Therefore where there would for instance previously be three vendor specialists using their own different proprietary technologies for achieving methodologies for their respective solutions, now the use of an open standard specification increases the pool of available vendor specialists for a given solution from one resource pool supplying knowledge or technology using that specification to three.

To ensure interoperability issues with suppliers, customers, partners and other related entities demand the need for optimisation of options which are of quality, durable and flexible in a corresponding environment where risk is reduced. Adopting an open standard increases options that lower risk in many ways.

The greater the optimisation and accessibility of the infrastructure built through an open standard, the greater the demand for innovation leveraging it. Continuous improvements can be driven until there is a need for a replacement of another new open standard, whereupon another door can be opened to collaboration on migration and interoperability.

By its nature of setting the open standard process through common open dialogue, communication is streamlined, allowing all end-users (educational or corporate institutions) to apply the concept. It also achieves a higher productivity from such users when compared to operating with closed concepts. Since an open standard is developed in a collaborative environment with open participation in the standard setting process, widespread and early open public and peer review becomes natural. This in turn increases early identification and resolution of potential problems which usually leads to higher quality results and better public reassurance in comparison to proprietary options.

As an open standard is supported by many suppliers, they are more durable by nature as compared to any more limited vendor solutions. Over the long haul, there is also more probability of the availability of support and continuous improvement. By nature, an open standard is not subject to a single vendor's interest but are more reflective on the demands of users, making them more durable.

Example

An example provided by the OpenStandards.net organisation in this regard is the use of the Structured Query Language (SQL) which is used throughout the relational database industry by Oracle, Microsoft and IBM as no single vendor has sufficient control to replace it.

Additionally, as technological progresses over time, proprietary solutions tend to be isolated as is shown by the early CompuServe and prodigy networks which have disappeared while the internet is growing at a phenomenal rate.

Furthermore, the fact that an open standard is supported by various vendors provides the end-user more independence from any one single vendor who might, absent open standard specifications, require the end users to rely on its own proprietary standard. This would in turn reduce end-user choice and competition. This is distinguished from de facto industry standards which encourage such end-user dependence. Increasing vendor options also result in reducing vendor costs and in reducing end-user risk, since such risk is transferred from a single vendor to multiple vendors implementing the same open standards.

Consequently, businesses developed around open standards benefit from a cost reduction, speedier market entry and an increase in market adoption and acceptance. This should result in an overall higher return on investment (ROI) as well as higher vendor independence. The competition between manufacturers and vendors creates pressure to produce and share improvements, with overall improvements for end-users.

4. Controversies regarding open standards

While there is a general understanding of the benefits of open standards, and even certain legal dispositions which mandate their use or implementation, in practice the situation is more complicated, because there are several forces pushing against the use of open standards, in particular proprietary (non-free) software and technology manufacturers who either have an interest in owning or controlling the specification of standards, or are interested in NOT implementing standards to maintain user lock-in.

4.1. Non-standard products

The most obvious area of conflict in relation to standards is that of vendor lock-in when using non-standard formats or protocols – made possible due to a dominant position or other factors (such as a copyright or patent right) of a vendor, whereby the vendor uses the economic or legal factors to leverage and "impose" de facto the use of a proprietary / closed standard.

> The typical example of this has been document formats in Microsoft® products, such as .DOC and .XLS. Microsoft's dominant position in the office suite market has created a "de facto" standard for document formats – to the point, for example, where bidders had to use these formats to submit bids for public contracts. The argument being that everyone needs to purchase Microsoft products to be able to create, read and exchange documents with third parties. This is obviously no longer the case, as software from other sources, such as OpenOffice.org, can read Microsoft formats (after significant investment in legitimate reverse engineering of those formats).

This is also visible in the strategy of "adopt and extend", whereby a vendor adopts a standard but then extends it with proprietary extensions, requiring thus the purchase and use of the vendor's products if one wanted to interoperate with this vendor's implementation or use the resulting files (e.g. regarding formats).

This may conflict with law regarding anticompetitive behaviour, which we comment on after reviewing the Intellectual Property Right issues pertaining to standards.

Example

Examples of this are CIFS (Common Internet File System), which gave rise to a European Commission investigation, and Kerberos extensions.

See Wikipedia "Embrace, extend and extinguish" for a controversial discussion and more examples.

4.2. Copyright and patent rights

There has been a lot of controversy and debate over the conflictive relationship between standards and "intellectual property rights", which in this case we include copyright and patent rights.

These rights are involved in two manners.

- **Copyrights**: A standard specification is a work protected by copyright (generally of the standards organisation that promulgates the standard,

but also potentially members of the work groups that participate in the process or submitting a specification as a standard). There is debate therefore whether:

– The organisation should be entitled to charge fees for accessing, reproducing and distributing the work that embodies an open standard.

– An implementation of the standard is a derivative work of that standard, and thus subject to authorisation by the rights holder of the standard.

• **Patents**: A standard specification defines a method or procedure on how to do something, and thus can fall squarely within the area of patentable subject matter. Thus any person having patent rights over the method specified by the standard can prevent anyone from implementing the process without licence.

Standards and patents, in particular, are intrinsically linked, as they both aim to encourage invention and creation through disclosure. To encourage publication or disclosure of breakthroughs which would in turn benefit the public, the government grants a patent owner with exclusive rights (monopoly) to his invention over a limited time. On the other hand, standards are also related to disclosure – they establish a common ground, promote interoperability and competition for the public benefit, facilitating customer choice between various products and services; and enable the exchange of information between one another without problems.

Although both benefit the public, upholding one deprives the other function.

Regarding patents and de facto standard, see the debate on GIF formats and Unisyst, commented.

The European Commission recognised that IPR owners and the beneficiaries of standards should be protected alike. However the common argument is that by allowing patents on standards, a monopoly is granted over part or all of the specification to certain private parties, a monopoly that includes the right to block implementation by other parties. Therefore the initial good intention in granting patents to encourage innovation for the public benefit might in the end lead to the prevention of further innovation down the line, when it prevents others from marketing their innovation just because it implements or interacts with the original invention.

The only way to avoid the patent is to create products or processes that circumvent them – thus falling into non-compliance with regard to the standard.

Other types of specifications are also sometimes referred to as standards and "belong" exclusively to organisations that own the copyright to the specification. As such, any right to the use of the specification can only be owned under restrictive contractual terms and are therefore not considered fully "open". For example, the rules for standards published by the major internationally

Supplementary content

For further reading, see: Analysis on balance: Standardisation and Patents at the FSFE site.

recognised standards bodies such as the IETF, ISO, IEC, and ITU-T permit their standards to contain specifications whose implementation will require payment of licensing fees.

4.3. Striking a balance?

In an attempt to mitigate the conflict and to balance the mutual benefits of standardisation and patents/copyright, and in particular to control the use of patent granted monopolies, the standardisation community have suggested adopting the "Ex-Ante Disclosure" mechanism and (F)RAND regime discussed further below.

•   Declarations and Ex-Ante Disclosure

If a specification or method proposed for a standard is covered by a patent or copyright right, the parties involved in the standardisation process are supposed to use the ex-ante disclosure mechanism which obliges them to disclose the existence of an IP right over a specification and the licence terms relating to it, otherwise the specification would not be included in the standard.

> See for example, ETSI[2] and ITU[3] sites.
>
> [2]See information on how to declare IPR and on ex ante disclosures at the ETSI site.
>
> [3]ITU also includes disclosure in its patent policy.

This theoretically allows members of the process to review the terms (or summary) and determine if they are acceptable or beneficial for the standard or not.

One criticism of this approach regards what are in fact acceptable licensing terms in these circumstances? They tend to vary and often prove to benefit corporations with a large patent portfolio as compared to the economic majority represented by SMEs which has no say regarding the acceptability of the terms imposed (see below on FRAND).

This has raised serious arguments over the membership of standardisation committees and organisations, as large commercial entities leverage their power to participate and propose technologies or specifications over which they have rights as an eventual standard.

•   (F)RAND

In reality, most standardisation bodies appear to opt for mere voluntary disclosure with assurance from other parties to approve RAND or FRAND ("Fair, Reasonable and Non-Discriminatory") terms for licensing patent rights on standards and not to exercise their exclusive monopoly rights as patent holders. In other words, (F)RAND generally amounts to a loose assurance to compulsory

licensing of their patent rights upon request. This was seen to ensure the right owner the opportunity to receive a reasonable return from his patent rights, and rewarding his innovation, and the time and creative effort.

A (F)RAND licence is sometimes imposed when joining the standardisation body, through membership rules. Participating companies having IP rights on technologies which become essential to the standard agree to equally allow other groups to implement the standard and license them those patents on reasonable charges, hence allowing competition between multiple companies which implement the same standard.

However a number of problems arise: What is reasonable licensing terms and for whom, since such terms vary depending on many factors e.g. commercialisation policies, whether or not a company has stake in the relevant market.

Another criticism is the usual non-perpetual nature of the licence, thus holders of patents on additional claims are free to enforce their patent terms in whichever way they like, including against existing (legitimate) implementations on the standard (the latter of which is in fact legitimate under the patent system). As a consequence, there is substantial uncertainty under the (F)RAND regime which invariably favours large companies which are better able to deal with such uncertainties, as compared to SMEs.

> A further critic is that even (F)RAND terms linked to zero royalties (or are royalty free) discriminate against Free Software since they do not allow sublicensing permitted by usage of Free Software (bearing in mind that the basis of Free Software or Open Source is that every living person or legal entity can be a user, developer, distributor or any of the combination.

FRAND terms also create an uneven playing field, for example in situation of public tenders requiring compliance with patented standards, whereby one bidder, not holding the IPR on the standard, has additional costs over the IPR holder bidder. This reduces or excludes competition.

4.4. Potential breach of (EU) Competition Law

Competition issues come into play because if a de facto or patented standard becomes a required specification, any operator without the IPR to be entitled to implement the standard would have its hands tied in the sense that it will have no choice but to license the IPR, at additional cost.

Free participation in the market is therefore not possible, or only on terms that are not commercially viable to the market entrant, and this could lead to market foreclosure or unfair terms of participation, resulting in possible breaches of the EU competition law: either Article 101(1) (formerly Article 81(1) EC) or the EU Treaty or Article 102 (Formerly Article 82).

- Article 101(1) prohibits agreements which prevent, restrict or distort competition within the Common Market and which affect trade between

Member States, unless they are capable of exemption under Article 101(3). Agreements regarding licensing terms – between participants or stakeholders within the context of a standardisation process – could fall foul of this provision.

• Article 102 prohibits the abuse by one or more undertakings of a dominant position within the market or in a substantial part of it which affects trade between Member States. Abuses can include imposing unfair or discriminatory terms, tying, bundling or exclusionary behaviour.

Any individual or collective dominance of the existing standards "owners" or participants which result in dictating discriminatory behaviour or constructive refusal to supply where the terms of participation would not be commercially viable, etc. would breach Article 102 of the EU Treaty.

Exemption is however granted under Article 101(3) where the agreement (e.g. relating to the standard) contributes to improving the production or distribution of goods or to promoting technical or economic progress, whilst allowing consumers a fair share of the resulting benefit. The said restriction must not be indispensable to the attainment of the objectives in question and not substantially eliminate competition for the products in question.

• For a US view, see William M. Hannay: "United States Antitrust Law Regarding Standard Setting Bodies", presentation at the Joint session Competition Law / IP Commission on The Interaction between Intellectual Property and Antitrust Law, UNION INTERNATIONALE DES AVOCATS.

• For the EU, see papers from the EC sponsored "IPR in ICT standardisation one-day workshop".

5. The Future Way Forward?

It might be a long while before a remedy is really workable in the patent and standardisation situation and where a consensus is reached between government, SME, free technologies and large corporations. In the interim, several issues have been highlighted as partial measures to ensure the full benefits of standardisation:

*   Interoperability. As we have seen, interoperability (either at applications level or on file formats) is one of the main objectives of standards. A proposed solution, similar to the interoperability carved-out in copyright law, is to provide that patent rights cannot limit the creation of interoperable products.
*   Competition: it would be favourable to determine the conditions in which the authorities would consider proprietary manufacturer/vendor IPR licensing terms and an approach to standards as illegal anticompetitive behaviour.
*   IPR policies. The policies of standards setting organisations should require non-discriminatory royalty-free licensing of any IPR over a standard, enabling any business model (including free software licensing based models) to implement the standards and participate in the market.
*   Government procurement: as a way of putting pressure on the market to move towards true interoperability and competition, rules regarding public tenders should ensure technological neutrality and require compliance with standards that are fully open (e.g. not subject to IP restrictions); and not rely on "standards generally accepted in the industry" or "used by citizens", which can be encumbered. This would enable a participation of all potential players in the market on a level playing field.

A key issue is that open standards are the basis for creating technological, economic and social ecosystems. Standards development and the ecosystem around open standards amount to a single community of interests, with interoperable or interchangeable products that allow vendors to compete on the innovation, not the standard. But ecosystems cannot rely on vague IP policies – even so-called RAND – whose general purpose is to limit, exclude or just to enable the rights holder to make economic profit from controlling entry on the market. The free software movement has proved that collaborative methods are based on free and open source licensing (and not much more). Conversely, restrictive licence agreements are anathema to collaborative methods: collaboration requires complete freedom of distribution and no barriers at all.

Further reading

*   Websites:

http://www.openstandards.net

http://perens.com/OpenStandards/Definition.html

http://progfree.org/index.html

- Patents and standards. FSFE. http://fsfe.org/projects/os/ps.en.html
- Workship papers from the EC sponsored workshop: "IPR in ICT standardisation", at http://ec.europa.eu/enterprise/newsroom/cf/itemshortdetail.cfm?item_id=3371
- Pat Treacy and Sophie Lawrance, "*FRANDly fire: are industry standards doing more harm than good?*" Journal of Intellectual Property Law & Practice, 2007

THIS BOOK CONTAINS FUNDAMENTAL INFORMATION FOR THOSE WHO WANT TO UNDERSTAND FREE SOFTWARE AND HOW TO CONTRIBUTE AND BENEFIT FROM IT IN A SAFE AND LEGAL WAY. CONCEPTS LIKE EXISTING LEGAL SYSTEMS OF SOFTWARE PROTECTION – COPYRIGHT, PATENTS, TRADEMARK AND KEY CONCEPTS LIKE COPYLEFT AND FREE LICENSES – WILL PROVIDE A GENERAL BACKGROUND UPON WHICH PRACTICAL SKILLS FOR DIFFERENT CONTEXTS CAN BE BUILT.

THIS MATERIAL AIMS TO PROVIDE THE KNOWLEDGE AND TOOLS THAT ARE NEEDED TO ASSESS THE POSSIBLE LEGAL ISSUES THAT CAN ARISE IN A FREE TECHNOLOGY ENVIRONMENT. IT WILL PROVIDE THE READER WITH THE INFORMATION NEEDED TO ANSWER TO COMMON QUESTIONS AND DOUBTS, AND TO TAKE THE RIGHT DECISIONS FROM A LEGAL PERSPECTIVE.