The Challenge of the Law to Electronic Commerce

Rolin Jacquemyns, Laetitia; Dusollier, Séverine

Published in:
Electronic Commerce : Opportunity and Challenges

Publication date:
2000

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

This article has been published in Syed M. Rahman, & Mahesh S. Raisinghani (ed), *Electronic Commerce: Opportunity and challenges*, IDEA Group Publishing, United States, 2000, p. 383-410

THE CHALLENGE OF THE LAW TO ELECTRONIC COMMERCE : THE EUROPEAN UNION INITIATIVES

Séverine Dusollier & Laetitia Rolin Jacquemyns

Researchers, Centre de Recherches Informatique et Droit,

(Centre of Research in Computers and Law), University of Namur, Belgium

INTRODUCTION

In the Communication on Electronic Commerce of 1997[1], the European Commission stressed that "*in order to allow electronic commerce operators to reap the full benefits of the Single Market, it is essential to avoid regulatory inconsistencies and to ensure a coherent legal and regulatory framework for electronic commerce*".

The electronic marketplace has a crucial need to know *"the rules of the game"*[2] in order to carry out electronic commerce. Therefore, the regulatory framework has to be clear, stable and predictable, both to enable e-commerce operators to face all challenges raised by the development of new products and services and to ensure the trust and confidence of consumers in the new electronic supermarket. These are the main objectives of the legislative action of the European Commission[3] which has, in recent years, laid the foundations for a consistent setting of the legal scene for electronic commerce in Europe. It is worth recalling that the action of the Commission has been and should be guided by the key principles of the EC Treaty, particularly by the concern for the Internal Market and the enhancement of the circulation of products and services. A clear consequence is that any regulatory intervention of the Commission should be directed to a further harmonization or clarification of the existing rules in order to lift the uncertainties and discrepancies in national policies which might impede the free circulation of electronic goods and services. Other key concerns of the European Commission are to refrain from over-regulating electronic markets and businesses and to remain open to a self-regulatory approach and alternative dispute resolution. This last guideline is particularly followed in the recent Draft Directive on electronic commerce[4].

The European Commission couples its legislative efforts with an overwhelming number of R&D projects that are developing new tools, technologies and services for electronic commerce. Within this framework, the ECLIP (Electronic Commerce Legal Issues Platform) project seeks to set up a platform on the legal issues of electronic commerce with the objective of providing legal support to EC-funded RTD projects on any issue of law linked to electronic commerce, thereby stimulating expertise and increasing general awareness of the existing or recommended legal framework of electronic commerce[5].

Other objectives of ECLIP consist in analyzing the current European legal framework and the technology available to be taken into account when launching an electronic commerce initiative, and of ensuring the early integration of the legal requirements in technological tools . This enables the lawyers to develop a techno-legal thinking that integrates technological features in legal solutions and principles. The ECLIP project promotes general and specific awareness among developers of legal issues on electronic commerce through publications, workshops, conferences, and animation of web sites.

One key aim of the project is to produce a global overview of the legal aspects of electronic commerce with a view to making recommendations to the EC. Such recommendations have already been addressed to the Commission in the field of user protection, privacy-enhancing technology, privacy-compliant browsers, alternative dispute resolution, labelling systems, electronic contracting and digital copyright protection.

ECLIP started in 1998 and is likely to go on until the end of 2002. Its main partners are five university research centers specialized in information technology law, i.e. the University of Namur (Belgium), the Queen Mary and Westfield College of London, the University of Münster (Germany), the University of the Balearic Islands (Spain) and the University of Oslo[6].

The purpose of this chapter is to provide an outline of the regulatory framework that the European Union has started to set up for electronic commerce. Some issues that the European policy-maker has to consider particularly are the key questions that any e-commerce developer has to cope with in the different steps of the development of his activity, from the establishment of his business, the advertising and promotion of his products, the selling of goods and services, to delivery and payment. These are the different sections we will address.

SECTION 1. THE EUROPEAN REGULATORY FRAMEWORK AT A GLANCE

A key measure for preventing the Member States from adopting a fragmented approach in the field of regulation of information society is the Directive of June 29, 1998 laying down a procedure for provision of information in the field of technical standards and regulations[7] (hereafter the 'Transparency Directive'). This text imposes Member States to notify the Commission and other Member States of any draft rules and regulation activity they undertake in the field of information society services. This transparency mechanism launches a process of making comments and giving opinions on aspects of the draft which may hinder trade, the free movement of service or the free establishment of service providers, which can lead to a postponing or modification of the proposed measure. This directive also lays down a definition of the information society services which will be used by subsequent relevant directives, i.e. "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*"[8].

Other key legislative acts are the Directive on the protection of consumers with respect to distance contracts[9] (hereafter the 'Distance Contracts Directive), the Directive on the legal protection of services based on, or consisting of conditional access[10] (hereafter the 'Conditional Access Directive'), the Directive on the legal protection of databases[11] (hereafter the 'Database Directive'), the Directive on the protection of personal data[12]. The European Union is in the process of adopting a number of other relevant directives such as the Proposal for a Directive concerning the distance marketing of consumer financial services[13] (hereafter the financial services Draft Directive), the Proposal for a Directive on certain legal aspects of electronic commerce in the internal market[14] (hereafter the 'E-commerce Draft Directive'), the Proposals for a Directive on the business of credit institutions[15] and for a Directive on electronic money[16] (hereafter the 'electronic money Draft Directives'), the Proposal for a Directive on a common framework for electronic signatures[17] (hereafter the 'Electronic signature Draft Directive), the Proposal for a Directive on the harmonization of certain aspects of copyright and related rights in the Information Society[18] (hereafter

the 'Copyright Draft Directive') and the proposal for a Directive aimed at establishing a clear regulatory framework for the marketing of financial services at a distance within the Single Market (hereafter the 'Financial services Draft Directive[19]') Although such texts are not yet enacted and thus might be subject to further modifications, they already highlight the position of the European legislators. We also note that most of the above mentioned Directives are minimum harmonization Directives, which means that the member States remain free to transpose the text in a more consumer protective way in their national legal framework. Therefore, for the purpose of this overview, attention should be paid to the fact that main provisions will not be binding as such, either because they are still in a draft stage, either because the European States may transpose them in a slightly different way. Nevertheless, we think that this outline might be of some interest to anyone who seeks a better understanding of the process and views of the European policy in that field.

Non-binding texts , such as Communications, Recommendations or Resolutions can also be of great importance in understanding the concerns and inclinations of the European legislator. They will be mentioned and considered where relevant.

SECTION 2 . APPLICATION OF EUROPEAN REGULATORY FRAMEWORK TO E-COMMERCE TRANSACTIONS

A first point of this chapter would be to define in which cases the European regulatory framework is applicable to electronic business. Determining which national regulations apply to e-commerce transactions is one of the most difficult and delicate questions of transglobal electronic networks. Legislative and case law answers are rare. One difficulty arises from the fact that some activities can occur in different territories, from setting-up a website, technical management, business management, hosting, access to network, to the making of contracts, commercial communications and delivery. The key question is to know with which national policies the activity has to comply. This is a matter for the national courts to determine - if they have jurisdiction over the litigation - and which law is applicable, by using rules of international private law. This field of law has been early on the object of the European harmonization. Recent directives on information society have specifically addressed the issue as well.

We can infer from the present regulatory situation that e-commerce operators would be under the jurisdiction of relevant EU Member States laws in the following cases :

- In the case of contracts, the Rome Convention of 1980 on the law applicable to contractual obligations[20] would still be applicable to information society contracts. The main rule of the convention is twofold. On one hand, the parties have the freedom to choose the law applicable to the contract. It is thus useful to insert a clause specifying the law applicable to eventual litigation in electronic contracts (software license, access to databases, sales contract, etc.). When dealing with consumers, the Convention nevertheless provides a prohibition to contract outside the mandatory rules of the country where the consumer normally resides. This rule applies only if a specific publicity and/or a specific invitation was made to the consumer in his country and if he accepted it there; if the other party or his agent received the consumer's order in that country; or if transborder shopping trips have been organized by the seller. Whether advertising products or services online should be regarded as a specific publicity directed towards consumers is still controversial. Some factors, such as the language used, the use of individual emails, targeted advertising tailored to the profile of the consumer, and any other factual elements indicating that the advertising is specific, can imply the application of the

derogation from the rule of free choice of law in the contract. In concrete terms, since most of the regulatory framework of consumer protection is mandatory in Europe, it would mean that the consumer would retain the rights granted by such protection if the law of the contract does not provide the same level of protection as that of his own country.

On the other hand, in the absence of a choice of law, the contract would be under the jurisdiction of the law of the country with which the contract has the closest connection. This connection is presumed to be with the country in which the party which has to undertake the characteristic performance of the contract has its residence. This presumption is rebuttable, i.e. subject to the proof of contrary, for instance if it appears that the contract is more connected to another country. But in the case of sales, the delivery of the product is often regarded as the characteristic performance of the contract, which would entail the application of the law of the seller, except when dealing with the consumer. In this last case, the convention imposes the application of the law of the country of habitual residence of the consumer. This would be the case for instance for a software license if the licensee intends to use the software for private purposes which fall outside his business[21].

This general rule of the Rome Convention for protecting consumers is coupled with article 12 of the Distance Contracts Directive that states that the consumers cannot waive the rights granted to them by the national laws transposing the Directive. But above all, contractual choice of the law of a non-EU country cannot have the consequence of depriving consumers of the protection granted by the Directive, if the contract has a close connection with the territory of at least one Member State, e.g. because the consumer and the supplier are located within the Community, or the consumer is located within the Community and his order is managed and carried out by an European agent of the supplier.

- The Data Protection Directive imposes its application[22] when the processing of personal data is carried out in the context of activities of an establishment of the controller on the territory of one Member State, or when the controller, not established within the Community, makes use - for the purpose of processing personal data - of equipment, automated or otherwise, situated on the territory of one Member State, unless such equipment is used only for purposes of transit through the territory of the Community. It is still discussed whether the use of cookies or other types of technology placed on the hardware of users and the processing of personal data should be regarded as the use of equipment within the European Community[23]. This rule of applicable law should be of great importance for e-commerce operators located outside EU, namely in the United States. Should they collect and process personal data through the use of equipment (such as an European server or a cookie), they would have to comply with the protective provisions of the personal data protection directive.

- In copyright matters, the question of applicable law is very delicate and partially unresolved[24]. Beyond contractual matters which enter the scope of the Rome Convention (see above), other rules apply to the existence and scope of protection of copyrighted material. First of all, the copyright protection will be granted under the provisions of the domestic law of the country of origin, i.e. the country where a work was first published.

  Secondly, article 5(2) of the Berne Convention states that "*the extent of protection, as well as the means of redress afforded to the author to protect his rights, shall be governed by the laws of the country where protection is claimed*". This law of the protecting country is the law of the

country where the work is exploited or used. Let's take an example in electronic commerce. If a piece of music is digitized and uploaded to the Internet, the law of the country in which the uploading occurred will be applicable to the issue as to whether the uploading belongs to the exclusive right of the copyright owner. This law is the law of the protecting country. If a work is communicated through the Internet, the situation is more complex, since the act of communication could be deemed occurring anywhere in the world[25].

- any information society service provider established in Europe to carry out e-commerce business would be under the control of the Member State where it is established. This is the solution preferred by the Draft e-commerce Directive. This rule's objective is to determine which Member States are responsible for ensuring the legality of the activities, thereby preventing restrictions to the free circulation of information society services within the European Union. Without being a rule of determination of applicable law, it can be said that the service provider established on the territory of one Member State will have to ensure that his activity complies with the relevant regulatory framework of this State, including the applicable Community regulation.

  The criterion is thus the establishment defined in article 2 of the Draft Directive as "*the pursuit of an economic activity using a fixed establishment forn an indeterminate duration"*. This definition focuses on the real nature and stability of the activity. It is also said that the presence and use of technical means and technologies required to provide the service (such as a website) do not constitute an establishment.

  This principle of country of origin would not apply[26] to intellectual and industrial property rights, emission of electronic money, direct insurance, contract obligations concerning consumer contracts and unsolicited commercial communication by e-mail. Such exemptions mean that in those cases other countries than the country of establishment have jurisdiction over possible illicit activities.

In conclusion, the European policies can be of great importance, even for e-commerce operators established outside the European Community. This is particularly true when dealing with consumers, when collecting and processing personal data in Europe or when exploiting copyrighted material inside the European Union.

SECTION 3 . INFRASTRUCTURE OF ELECTRONIC COMMERCE

Electronic commerce takes place in a converging environment where telephone, television and personal computers offer similar services, and creates new markets whose boundaries are fading away. This convergence of services and markets raises new legal issues, such as defining the regulatory framework to be applied thereto. Current regulations of the audio-visual sector, on one hand, and the telecommunications sector on the other hand are largely different and sometimes contradictory. Their convergence would not be an easy task. A recent Green Paper of the European Commission[27] on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation addresses numerous challenges, such as the relevance of regulations based on scarcity of spectrum, the blurring of boundaries between public and private activities, the likely overlapping of current regulations or the key issue of access to content.

As far as telecommunication is concerned, the European Union has been engaged in a gradual process of liberalization of the sector[28] for the past ten years. This has been fully completed as of 1st January 1998. As a result, the number of infrastructure providers and Internet access providers has continuously increased. A great number of directives constitute the architecture of this process : the services directive 90/388, satellites directive 94/46, the Directive on the use of cable TV networks for already liberalized telecommunication services 95/51, the mobile and personal communications directive 96/2, and so on.

Nevertheless, exploring those documents would go beyond the frame of the present chapter.

SECTION 4. ESTABLISHMENT OF A SERVICE PROVIDER

The European Union tends to acknowledge the establishment of an information society service provider without requiring any prior authorization or control procedure. The draft e-commerce directive would forbid Member States to provide such an authorization scheme which could impede the free establishment of e-commerce operators. This prohibition would apply to information society services, defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". Any procedure having basically the same effect would be prohibited as well. Therefore the access to the supply of products and services on the Internet would be facilitated. The provision is without prejudice (a) to authorization schemes existing in the telecommunications field and (b) to those which are not specifically and exclusively targeted at information society services. This last case covers the activities that require authorization or for which the operator has to justify he has the required professional qualifications, whether this activity is carried out in the real world or on the Internet. Some examples are travel agencies, insurance agencies, the sale of medicines, activity of lawyers, etc.

SECTION 5. INFORMATION TO BE PROVIDED

Everybody knows the famous sentence : "on the web, nobody knows that I am a dog". Indeed, in the information society age, it is not rare that a user has no idea or information about what is hidden behind the website he is browsing. Some websites prefer to stay anonymous, others neglect providing any information other than their email address. A recent US study carried out by the FTC showed that more than half the websites don't give any physical address or contact point.

With such a lack of transparency, the consumer or company might be reluctant to engage business with someone so physically invisible. In case of conflict, for instance if the delivered product is not the one requested or is defective, if the price is debited twice, one can wonder where complaints should be addressed. Is an email address sufficient ? And what if nobody answers to subsequent emails ? Where can one address a formal notice ?

Some techniques are developing in order to facilitate the identification and authentification of web sites and hence enhance the trust of users. Labelling web sites is one of such techniques, encouraged by the European Commission for that matter[29]. Labellisation results from an audit procedure assessing the compliance of the web site with a number of business, security and legal requirements. The label then posted on the website guarantees the compliance of the site with the requirements of which a list is hyperlinked to the label, thus enabling the user to check.

Along with the development of technical solutions from the electronic commerce market itself, the European Commission puts forward a regulatory response. Article 5 of the Draft e-commerce directive would compel information society services to identify themselves by providing the following information:

(a) the name of the service provider;

(b) the address at which the service provider is established;

(c) the address of the service provider including his electronic-mail address;

(d) where the service provider is registered in a trade register, the trade register in which the service provider is entered and any registration number in that register;

(e) where the activity is subject to an authorization scheme, the activities covered by the authorization granted to the service provider and the co-ordinates of the authority providing this authorization;

(f) as concerns the regulated professions, the professional body or similar institution with which the service provider is registered and the professional title granted in the Member State of establishment, the applicable professional rules in the Member State of establishment and the Member States in which the information society services are regularly provided;

(g) in the case where the service provider undertakes an activity that is subject to VAT, the VAT number he is registered under with his fiscal administration

The information in question must be easily accessible in a direct and permanent manner to the recipients and competent authorities. It is said in the comments of this article that an icon or logo inserting on the web pages with a hyperlink to a page containing the information would be sufficient to meet the requirement.

Supplementary information should be given to consumers when contracting on-line. It will be examined below.

SECTION 6 . COMMERCIAL COMMUNICATIONS

The European Union has given particular consideration to the legal issues arising from on-line commercial communications, both from a consumer protection's point of view and from a business-to-business point of view.

In its communication of March 4th, 1998 on the follow-up of the Green Paper on Commercial Communications in the Internal Market[30], the Commission has decided to refrain from adopting a binding instrument for commercial communications, whose objective would be for instance an harmonised prohibition of advertising of some products (e.g. tobacco, drugs, etc.), or an harmonised framework of specific requirements related for instance to language, to information to be provided.

Instead, it proposes the application of a specific methodology to assess the possible effects and proportionality of a commercial communications measure. The application of this methodology would prevent any national restrictions on communications but those based on public interest objectives. The

Commission also intends to set up a database with national and Community regulations and self-regulatory codes in this field.

The Draft e-commerce Directive seeks to regulate further commercial communications by subjecting them to some transparency requirements. Commercial communications**,** defined as *"any form of communication designed to promote, directly or indirectly, goods, services or the image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a liberal profession*", would have to comply with the following requirements :

1. the commercial communication must be clearly identifiable as such;

2. the natural or legal person on whose behalf the commercial communication is made must be clearly identifiable;

3. promotional offers, such as discounts, premiums and gifts, where authorized, must be clearly identifiable as such, and the conditions which must be met to receive them must be easily accessible and be presented accurately and unequivocally;

4. promotional competitions or games, where authorized, must be clearly identifiable as such, and the conditions of participation must be easily accessible and be presented accurately and unequivocally.

Moreover, the article 7 of the draft states that unsolicited commercial communication by electronic mail must be clearly and unequivocally identifiable as such as soon as it is received by the recipient.

Besides, three European Directives offer consumers the possibility to oppose obtrusive commercial communications :

- the Directive on the protection of individuals with regard to the processing of personal data[31] whose article 14 states the right of data subject to "*object, free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing";*

- another personal data protection directive has been adopted in the field of telecommunication. Its article 12 prohibits the unsolicited calls for purposes of direct marketing, unless the consumer has given his consent;

- the Distance contracts directive lays down that "*means of distance communication which allow individual communications may be used only where there is no clear objection from the consumer*".

Both data protection and distance contracts directives establish the principle of opt-out where individual distance communications are allowed only in the absence of a clear objection from the consumer.

SECTION 7 . CONSUMER PROTECTION

A recent directive governs distance selling contracts between consumers and suppliers. In the initial version, the financial services were excluded from the scope of application of the Directive. Recently, the Commission proposed a financial services Draft Directive that would modify the distance selling contracts directive to add the financial services that will be regulated by specific provisions. We will mention, when relevant, the specific regulations of the financial services. But it is not clear as yet how the Commission will combine both of the texts relative to distance contracts. It means that the interpretation given in this article could change rapidly concerning the financial services and their integration in the distance contract Directive.

Distance contracts cover "*any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who for the purpose of the contract, makes exclusive use of one or more means of distance communication*[32] *up to and including the moment at which the contract is concluded* ".(article 2.1.) From this definition and from the areas that are explicitly excluded from the scope of the directive[33], it appears clearly that the "on-line delivery and/or distribution of materials" is covered by the directive. Main rules laid down in the Directive are :

Prior Information: In good time prior to the conclusion of any distance contract, the consumer must be provided with information[34] concerning :

(a) the identity of the supplier and, in cases requiring payment in advance, his address,

(b) the main characteristics of the goods and services;

(c) the price of the goods or services including taxes,

(d) delivery costs, where appropriate,

(e) the arrangements for payment, delivery or performance,

(f) the existence of a right of withdrawal,

(g) the cost of using the means of distance communication, when it isn't calculated with the basic rate,

(h) the period of time for which the offer remains valid,

(i) the minimum duration of the contract.

Concerning the financial services, the content of the prior information is extended to add more precision regarding the price of the service and, if need be, the way to calculate it.

For contracts that are intended to be entered into on the Internet, it is best that this type of information be included on a website in a clearly accessible manner. An hyperlink to an information page could be sufficient on the condition that it refers to information in an on-going way and can be accessed at any stage of the website browsing.

Written confirmation of information : Article 5 provides : *"the consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Art. 4(1)(a) to (f), in good time during the performance of the contract, and*

at the latest on delivery .

In any event the following must be provided :

- *written information on the conditions and procedures for exercising the right of withdrawal,*
- *the geographical address of the place of business of the supplier to which the consumer may address any complaints,*
- *information on after-sales services and guarantees which exist,*
- *the conditions for canceling the contract, whether it is of unspecified duration or of a duration exceeding one year. »*

Right of withdrawal: As a rule, for any distance contract, the consumer will benefit from a period of at least 7 working days in which to withdraw from the contract without penalty and without giving any reason. The supplier will then be obliged to refund the sums paid, free of charge[35]. However, an exception is provided, which will probably apply to some cases of on-line distribution of protected material: Unless the parties have agreed otherwise in respect of certain types of contracts, such as for the provision of services, if the performance has begun with the consumer's agreement, before the end of the seven working day period, for the supply of newspaper, periodicals and magazines or for the supply of audio or video recordings or computer software which were unsealed by the consumer. In the case of the financial services, the right of withdrawal is excluded for services concerning change operations, money market instruments, transferable securities, UCITS and other collective investment schemes, financial futures and options, exchange and interest rate instruments, non-life insurance from a duration under 2 months, and the complete fulfilment of the contract before the consumer uses his/her right of withdrawal.

Performance: Again, unless the parties have agreed otherwise, the supplier must execute the order within a maximum of thirty days from the day on which the consumer forwarded his order to the supplier[36].

SECTION 8 . ELECTRONIC SIGNATURE

Doing electronic transactions requires the acknowledgment of the formal validity of digital files and documents. Yet, most European countries still impose that documents be made or at least proven in writing and validated by a hand-written signature. On the electronic networks, the issue of the evidence and authenticity of the documents and parties has been largely discussed so far. A number of countries are in the process of enacting a legislation that provides the equal value of hand-written and digital signatures. Besides the work already done by the UNCITRAL[37] and the OECD, the European Commission has proposed in a recent draft directive the establishment of a common framework for electronic signature.

Its objective is twofold :

- to prevent Member States from denying an electronic signature legal effect, validity and enforceability on the sole grounds that it is made electronically;

- and to ensure the free circulation of certification services and certificates within the European Union.

According to the Proposal, Member Sates shall recognize the validity and the evidentiary value of electronic signatures which are based on a qualified certificate issued by a certification service provider who satisfies a number of requirements set out in the Proposal. Certificates would be considered as qualified if they include certain mandatory information, such as :

- the identity of the certification service provider,
- the name of the holder and his specific attributes,
- the signature of the verification device,
- the time limit of validity,
- the electronic signature of the certification service provider,
- the identity code of the certificate.

The operators willing to engage in certification activities would have to fulfill certain conditions of trust and reliability as well. For instance, they would have to justify that they employ qualified personnel, that they take measures against forgery of certificates and confidentiality, that they have the financial ability to pay damages if they were to be found liable. They also should provide consumers with some prior information before contracting and refrain from storing private keys, except if the consent of the holder is given. These requirements will not be mandatory for the exercise of their activity but the certificates they will deliver will gain greater legal force.

Other provisions of the Proposal rules the liability regime of certification service providers, data protection requirements and the guarantee of the free circulation and mutual recognition of certificates and certification services.

SECTION 9 . ELECTRONIC CONTRACTS

Acknowledging the validity of electronic transactions is the necessary complement of the legal value of the electronic signature. This issue is the follow-up of the EDI question that had arisen in the mid-70s and has similarly showed the lack of legal recognition of the electronic contracting. Normally, the contract is formed between two parties when there is an actual consent to conclude such an agreement. The question arises whether clicking on an icon 'I accept' or 'I agree' amounts to the acceptance of the contract. Not only this question of the reality of the consent can be somewhat complex in an electronic process, but the evidence and validity of the electronic agreement can be difficult to reach in some countries which still impose formal requirements.

These are both obstacles that constitute the main background of the relevant provisions of the Draft e-commerce Directive[38].

Article 9 requires the Member States "*to ensure that their legislation allows contracts to be concluded electronically. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither prevent the effective use of electronic contracts nor result in such contracts being deprived of legal validity because of the fact they have been concluded electronically*". This article is formulated very broadly and seeks to cover any stage of the contractual process. This would mean that the Member States would have to assess and systematically review any rule which might prevent, limit or deter the use of electronic contracts. Not only the form requirements, such as an obligation to produce a 'paper', laid down in national legislation, but also any rule which might lead in practice to a difficulty to electronically contract would have to be reviewed and properly modified. The various stages of the contractual process to be considered are : the invitation to trade or the contract offer itself, negotiations, the offer or invitation to enter a contract, the conclusion of the contract, registration, cancellation or amendment of the contract, invoicing and archiving of the contract.

In concrete terms, no national provisions restricting the use of electronic media or electronic systems such as intelligent agents, weakening the legal effect of electronic contract or requiring formalities or conditions[39] that cannot be met by electronic means would be prohibited and should be adapted.

Some exemptions can be provided for instance for family law, succession contracts or contracts requiring the intervention of a notary or the registration with a public authority.

The problem of the consent to conclude the contract is ruled by a transparency and information system. Indeed, article 10 would impose that the service provider explain the manner in which the contract is formed clearly, unequivocally and prior to the conclusion of the contract. This information shall include:

– the different stages to follow to conclude the contract;

– whether or not the concluded contract will be archived and will be accessible;

– any available means of correcting handling errors.

This information shall not be mandatory between professional parties when otherwise agreed.

It will be a matter for Member States to lay down in their legislation that the different steps to be followed to conclude an electronic contract be set out so as to ensure that parties can reach a full and informed consent. Appropriate means should also be offered by the service provider for enabling the recipient of the service to identify and correct handling errors. Thus, the Proposal does not specify whether automated consent carried out by intelligent agents would be valid, neither the way in which contractual terms or webpages should be designed and presented.

Finally, the Draft Directive determines the moment when the electronic contract shall be deemed to be concluded, i.e. when the recipient of the service receives from the service provider, by electronic means, an acknowledgment of receipt of the recipient's acceptance, and confirms receipt of the acknowledgment of receipt. This latter step (confirmation of receipt) would probably be removed from the proposal in line with the amendments already adopted by the European Parliament. This will have the advantage of simplifying this intricate and rather non-practical rule. Other modifications are likely to be brought to this article 11, since the controversy has so far been intense on that point. The acknowledgment of receipt is deemed to be received and the confirmation is deemed to have been given when the parties for whom they are destined are able to access them.

This moment of conclusion of the contract is relevant to determine the moment when the contract becomes binding for the parties, the law applicable to the contract and any other modalities of the contract which might be determined by a time criterion. This issue was already crucial in other types of contracts concluded at a distance, for instance by telephone, fax or ordinary mail. The contract was considered to be concluded at different times according to the countries, which some relate to the sending of the acceptance letter, while others focus on the time of the receipt of the acceptance. Once adopted, the article 11 will settle these discrepancies amongst national laws in Europe.

SECTION 10 . ELECTRONIC PAYMENTS

To create an adequate legal framework for the electronic payments is one of the great challenges of the Internet regulation. First of all because there are different categories of payment and secondly because those payments sometimes use complicated technologies. The main categories of payment in Europe are the electronic money instrument and the credit card. It is important to mark the difference because those instruments are not exactly regulated in the same way and are designed for rather different purposes. The credit card has the advantage of being used world-wide and the tracability of its issuer ensures it an easier acceptance on the Internet. Moreover, it offers the possibility to make payments for larger sums.

The electronic money instrument is, on the contrary, designed for small to micro-payments, the trust it can inspire relies more on the complex technology it is based on. It has the following characteristics: the payment is made offline thanks to a technology that allows the storage of monetary units on a device that could[40] be either a chip card or a computer memory.

Credit cards.

The choice of limiting the analysis to credit cards and not speaking of some other payment instruments could appear arbitrary. But it seems that they are becoming now one of the most popular payment instruments used because of the development of security features like cryptography or digital signatures and certificates. Those applications will allow the credit card number to travel through the network safely.

There is a particular European text that is of great help for understanding the regulation of credit cards when they are used for cyber payments. It is the Commission recommendation (hereafter the recommendation) concerning the transactions by electronic payment instruments[41].

We note that a recommendation is not considered as a legal binding instrument, but it remains important to analyze and understand it because the Commission will conduct a survey to decide whether the recommendation has been sufficiently implemented in the different Member States, and if not will issue a Directive that will certainly be strongly inspired by the actual recommendation.

To be included in the scope of the recommendation, the electronic payment instrument must enable the holder to perform transfers of funds or/and cash withdrawals[42]. There is no particular disposition on the quality of the issuer that is defined in article 2 (e) as "*a person who, in the course of his business, makes available to another person a payment instrument pursuant to a contract concluded with him/her*". But he supports several obligations that relate on the one hand to the transparency of the conditions of transaction and on the other hand to the loss or theft of a payment instrument.

Prior to the transaction, to achieve the transparency, the issuer must for example[43]:

- Upon signature of the contract or in any event in good time prior to delivering an electronic payment instrument, communicate the contractual terms and conditions governing the issue and use of that electronic payment instrument to the holder. The terms indicate the law applicable to the contract.

- The terms set out in writing include at least

  (a) a description of the electronic payment instrument,

  (b) a description of the holder's and issuer's respective obligations and liabilities,

  (c) where applicable, the normal period within which the holder's account will be debited or credited,

  (d) the types of any charges payable by the holder.

  - the amount of any initial and annual fees,

  - any commission fees and charges payable by the holder to the issuer for particular types of transactions,

  - any interest rate which may be applied, including the way in which it is calculated;

  (e) the period of time during which a given transaction can be contested by the holder and an indication of the redress and complaints procedures available to the holder and the method of gaining access to them.

- If the electronic payment instrument is usable for transactions abroad (outside the country of issuing/affiliation), the following information is also communicated to the holder:

  (a) an indication of the amount of any fees and charges levied for foreign currency transactions, including where appropriate the rates;

  (b) the reference exchange rate used for converting foreign currency transactions, including the relevant date for determining such a rate.

There is also some information to be provided after the transaction, like for example a reference for identifying the transaction, the amount debited and the related fees or charges.

But the most interesting part of the recommendation concerns the repartition[44] of the respective rights and obligations of the issuer and the holder in case of loss or theft. Everything is organized around the moment of the notification of the loss or theft. In fact, the issuer must ensure that appropriate means are available to enable the holder to make the required notification, including ,when it is made by phone (which is currently the most common way), the provision of a proof that such a notification has been made.

Therefore, up to the time of notification, the holder bears the loss incurred as a result of the loss or theft of the electronic payment instrument up to a limit which may not exceed 150 EURO, except when he has acted with an extreme negligence or fraudulently, in that case no limit is applicable. What is meant by

extreme negligence is for example the recording of his/her PIN in an easily recognisable form or late notification. After the notification, the holder is not liable anymore for the loss arising except if he acted fraudulently. But there is one specific case where that regime is not applicable. It is when the payment instrument has been used without physical presentation or electronic identification (of the instrument itself) and the recommendation adds that the use of a confidential code or any other similar proof of identity is not sufficient to entail the holder's liability.

That specific provision has to be read in relation with the common use of the credit card number and the expiration date (without any signature) as a means of payment. If that mean is used by an intrusive third party after the loss or theft of the instrument, the holder will not be liable. Certain authors argue that such provision has to be viewed as a strong encouragement from the Commission to use digital signatures and certificates.

Electronic money instruments.

The European Commission has showed a particular interest in electronic money and is trying now to create a legal framework for its issuing that will open the electronic money business to non bank institutions by creating lighter conditions for the access to that kind of activity[45].

Beside the issuing, other aspects of electronic money have been regulated by another European text that is actually the European Commission recommendation concerning the transactions by electronic payment instruments. The electronic money instrument is defined as a reloadable instrument other than a remote access payment instrument, whether a stored-value card or a computer memory, on which value units are stored electronically, enabling its holder to effect transactions like electronic funds transfers or cash withdrawals[46].

The legal framework applicable to the electronic money instrument is not so far from the credit card one. But, according to the special nature of the instrument (limited value and pre-payment) the recommendation creates a strange system of a two levels application. The electronic money instrument is considered to have two main functions : a payment function and a loading function through remote access to the holder's account. Some dispositions are not applicable to the payment function like for example article 6 which contains the dispositions relative to the liability of the holder. It means that the notification-based regime will not be applicable to the payment made by an electronic money instrument. But the recommendation applies fully to the loading function.

There is also some specific provision such as the obligation for the issuer to provide the holder with the possibility of verifying the last five transactions made with the instrument and the outstanding value stored thereon. That system means that there is also an obligation to provide information subsequent to the transaction, made with the electronic money instrument.

Another specific provision puts the liability on the issuer for the lost amount stored on the instrument and for a defective execution of a transaction that are attributable to a malfunction of the instrument, the equipment or any other equipment authorized for use.

SECTION 11 . VAT REGIME FOR ON-LINE SALES[47]

Unlike direct taxation, the regulation of indirect taxation is within the competencies of the European Commission. It means that it is the Commission that now faces the challenge to adapt the indirect taxation to the digital world. The central problem arises from the fact that all transactions are passing through the network and can not be counted or supervised by any authority without considerable investments in time and money.

General notions

The following transactions shall be subject to value added tax[48] : the supply of goods or services effected for consideration within the territory of the country by a taxable person acting as such and the importation of goods." A taxable person means "any person who independently carries out in any place any economic activity (…), whatever the purpose or results of that activity. The economic activities referred to (in paragraph 1) shall comprise all activities of producers, traders and persons supplying services including mining and agricultural activities and activities of the professions. The exploitation of tangible or intangible property for the purpose of obtaining income therefrom on a continuing basis shall also be considered an economic activity".

Qualification of the transaction.

According to the qualification which will be given to the transaction, the burden of the tax will be supported by one or another party. The reason is that there are different rules according to the type of transaction made. There are two main categories of transactions which are the delivery of goods and the supply of services. Each of those main categories contains different sub-categories such as, in the case of delivery of goods, distance selling, delivery of goods with transport by the recipient, etc.

In a communication to the Council, the Parliament and the Economical and Social committee on electronic commerce and indirect taxation, the Commission stated the opinion that the goods ordered and delivered through the networks are to be considered as services. This communication is as yet the only action taken by a European institution to adapt the existing framework to electronic commerce.

Place of the transaction.

The general rule is that taxable services are taxed in the tax jurisdiction to which the supplier belongs[49], but this principle is subject to a lot of exceptions. The reason for the exception is to limit the "distortion of competition caused by tax differentials between tax jurisdictions in relation to purchases by those who are not permitted to set off the input tax credit[50]". The exceptions generally relate to intellectual services like transfer of copyrights or financial services.

For example, in the United Kingdom, the VAT may be chargeable on the provision of services if the place of supply is the UK. A UK customer who acquires certain intellectual services[51] may be treated as having been supplied with those services in the UK, even though the supplier may have no place of business in the UK.

Under these circumstances, a recipient (subject to the VAT) of such services would be required to charge VAT on the 'imported service' under the "reverse charge" procedure. According to this procedure, the recipient is required to account for input VAT, instead of the supplier[52].

The process of the reverse charge works only in two cases : when the supply is to a person who belongs outside of the European Union and when the supply is to a taxable person in another Member

State and for the purpose of that person's business[53]

The system of VAT in Europe is complicated and currently allows a lot of threats by way of electronic means for the transfer of information because it seems obviously difficult to control the transactions made on an open network.

SECTION 12 . PROTECTION OF PRIVACY

Data on users and consumers are a key asset in electronic commerce. Knowing the profile and interests of potential clients enables a company to reach relevant markets and people to offer them the products and services they might be looking for. Let alone that such data can be easily collected, processed and connected to other files when they have been given by the user when browsing the Internet, with or without his knowledge. There is no need to say that the threats to the privacy of Internet users are numerous. Moreover, this threat is also one of the primary reasons why a great number of people are still reluctant to use the web for buying goods or services.

Privacy has thus become one of the main concerns of the business and of users willing to carry out electronic transactions. Privacy-enhancing technologies are developing, technical standards seek to be privacy-compliant[54] and a greater number of operators display their privacy policy on their web pages.

The European Union has set up a coherent regulatory framework for protecting personal data and ensuring at the same time the free circulation of this data within the Internal Market. The key instrument is the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free circulation of such data[55]. Most European countries have already transposed the Directive in their national laws. A second directive has been enacted in 1997 in the specific field of telecommunications and complements the general directive[56].

'Personal data' are very broadly defined by the data protection directive as "*any information relating to an identified or identifiable person*". To determine whether a person is identifiable, account shall be taken of all the means reasonably likely to be used by the controller or by any other person to identify the person[57]. In an e-commerce environment, a number of data related to persons are collected and processed, for instance through conditional access systems, use of digital signatures, electronic ordering of goods or services. Other data might be considered as personal as well. This could namely be the case of a fixed IP address, which leaves its trace when the user is surfing, when coupled with facilities providing other identification of the user, such as cookie or data collected by a profiling agent, email address, etc. Nevertheless the question is very controversial.

The Directive imposes some obligations to the controller of the processing who is defined as 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. These obligations are the following:

1. personal data must be processed fairly and lawfully: this implies that the purpose of the processing must be transparent and clearly explicit and that the data subject should be informed of the collecting on data related to him and of the purpose thereof.

2. personal data must be processed for legitimate purposes : the criterion of legitimacy is not fixed and is left to the appreciation of courts or national data protection institutions.

3. personal data may not be processed in a way incompatible with the purposes for which the data are collected: such purposes have to be determined at the time of collection of data and can be extended to

other secondary purposes only in a compatible way : for instance, data collected in order to monitor the proper delivery of goods or performance of services ordered by a customer, should not be used for further marketing purposes, unless this purpose has been specified to the user earlier.

4. the processing of personal data can namely occur if [58]:

    - the data subject has unambiguously given his consent;
    - the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
    - The processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject.

5. Sensitive data relative to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex-life, can only be collected upon strict conditions.

6. Data must be adequate, relevant and not excessive as regards the purposes for which they were collected;

7. Data must be accurate and kept up to date;

8. data may only be kept as long as necessary.

9. the controller has to ensure the security of the data by adequate technical measures.

10. the controller must notify the processing to the national authority responsible for the supervision of the protection of personal data.

Finally, the Directive grants certain rights to the data subjects : the right to be informed of the identity of the controller and of the purpose of the processing, the right to get access to the data collected on him, the right to rectify data, the processing of which does not comply with the Directive, and the right to object to the processing for compelling legitimate reasons. This latter right does not have to be based on a justification when the purpose of the processing is marketing.

The Directive prohibits the transfer of personal data to non EU countries, except if the country of destination guarantees an adequate level of protection, if the data subject has consented to the transfer or if the transfer is necessary to the performance of a contract to which the data subject is a party. Due to the transfrontier nature of the electronic commerce, this general prohibition of transfer to third countries could be a problem. A solution for e-commerce operators concerned with the privacy of their clients is to ensure adequate safeguards with respect to the protection of personal data, for instance through contractual solutions or through codes of conduct whose principles would be compliant with the personal data directive.

SECTION 13 . COPYRIGHT PROTECTION

a) Introduction

In its Communication on the Follow-Up to the Green Paper on Copyright and Related Rights in the Information Society[59], the Commission announced that it intended to propose a number of harmonizing measures in the field of copyright and related rights with a view to adjust and further complement the existing legislative framework, where this is necessary for the proper functioning of the Internal Market and for bringing about a favorable regulatory environment for the development of the Information Society in Europe. Therefore, a draft Directive on the harmonization of copyright and related rights in the Information Society was proposed by the Commission in December 1997. This Draft Directive would complete the existing copyright harmonization carried out so far in the field of protection of software and databases, harmonization of the copyright duration, neighboring rights and lending and rental rights[60], thereby forming a coherent copyright regulatory framework in Europe, ready to face the information society challenges[61].

At the same time, it implements a significant number of the new WIPO Treaty obligations (resulting from the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty" adopted at the Diplomatic Conference of Geneva in December 1996[62]) on a Community level in parallel with the ratification of these Treaties by the Community. In some cases, the proposal goes beyond the provisions enacted by the WIPO Treaties by seeking to implement on a European scale former proposals submitted -but not adopted- to the Diplomatic Conference.

As set out in the Commission's Communication of 20 November 1996[63], harmonization is proposed for six elements :

- *the right of reproduction;*

The stake of the definition of the scope of the reproduction right[64] has always been fundamental for rightholders as for other actors involved in on-line delivery of copyrighted material, such as users, telecommunications operators, access providers, etc... Actually, the on-line transmission of works or performances protected by an intellectual property right implies a number of transient and technical electronic reproductions of works. Whether such reproductions are covered by the scope of the reproduction right as defined in most Member States is still uncertain, which justifies the necessity to provide for a harmonized definition of this right of reproduction.

The definition finally adopted in the proposal is : *" the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part."*

Such a definition conveys clearly that temporary and transient reproduction is subject to the exclusive right of the rightholder. Nevertheless, an exception to this reproduction right with regards to this particular technical reproduction is put forward in the article 5 (1) of the proposal, which states that "*transient and incidental acts of reproduction which are an integral and essential part of a technological process, including those which facilitate effective functioning of transmission systems, for the sole purpose of enabling use to be made of a work or other subject matter, and having no independent economic significance, shall be exempted from the right set out in Article 2"*.

This exception seeks to take into account the concerns of service and access providers concerning the incidental acts of reproduction. "Browsing", "caching" or transient fixations necessary for transmission through networks may thus not be restricted acts if they comply with particular requirements set out in art. 5(1)[65]. The transposition of this exception of temporary acts of reproduction will be obligatory for the Member States.

This provision applies also to the other rightholders recognized in the *acquis communautaire* (performers, Phonograms and film producers and broadcasting organizations, sui generis rightholders for databases) and the new WIPO Performances and Phonograms Treaty who benefit from the same level of protection for their works or other subject matter as regards the acts protected by the reproduction right.

- the right of communication to the public, including making available "on-demand" over the net;

Article 3 of the proposal sets out : *"Member States shall provide authors with the exclusive right to authorize or prohibit any communication to the public of originals and copies of their works, by wired or wireless means, including making their works available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them"*

One of the main objectives of this provision is to make it clear that interactive "on-demand" acts of transmission are covered by this right. Actually, the fact that individuals may have access to such services and request their transmission individually had raised a doubt as to whether such transmission was made to the *public* and not to a private person. This provision aims to settle this key question by providing that the *public* consists of individual *members of the public*.

- the right of distribution of physical copies, including its exhaustion

Article 4(1) of the Proposal provides authors with the exclusive right to authorize any form of distribution to the public - by sale or otherwise - of the originals and copies of their works. Both new WIPO treaties contain also an exclusive right of distribution, namely the right to authorize or prohibit the distribution of fixed copies as tangible objects (e.g. on paper, CD, CD ROM, tape, as opposed to on-line form). The distribution right does thus not apply to services in general or on-line.

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

This latter provision finally meets the view of the Diplomatic Conference which decided that it shall be a matter for Member States to determine the existence and the conditions of the exhaustion of the distribution right. Consequently, the Proposal has chosen the principle of community exhaustion while providing that the distribution right should not be exhausted after a first sale outside the European Union[66].

Exceptions to the reproduction right and communication to the public right

Article 5 harmonizes the limitations and exceptions to the reproduction right and the communication to the public right[67]. The list set out in this provision is exhaustive, which entails that national legal systems would not be allowed to maintain any exceptions to copyright other than those enumerated. But, apart from the exception for temporary reproduction mentioned above, the

implementation of these exceptions is only facultative. Thereby, it shall be a matter for each Member State to decide which exceptions he will transpose in its legislation. The harmonization foreseen by the proposal is thus relative, since after the transposition of the directive in national laws, the systems of limitations to copyright could still comprise a number of disparities from a country to another both in the actual exceptions in force as in their scope and interpretation.

The list of exceptions is very detailed and precise. The European Parliament has amended it so that a number of exceptions would be coupled with an obligation to provide the rightholders with a fair remuneration.

The list of exceptions is the following :

Article 5(2) sets out five exceptions to the reproduction right:

- Article 5(2) (a) allows Member States to maintain or introduce an exception for photo/print type reproduction ("reprography"), with a remuneration scheme.

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

- Article 5(2) (b) allows for exceptions regarding reproduction of audio and audio-visual material for private use and for non-commercial ends, but makes a distinction between the *analogue* private copy and *digital* private copy. This last one will not prevent the use of operational, reliable and effective technical means capable of inhibiting the copy. A fair remuneration should be attributed to rightholders for both types of copy.

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

  This exception does not apply to the communication to the public right. Thus, a library making a work available from a server to users on-line should and would require a license of the rightholder or his intermediary and would not fall within a permitted exception It is stated in the Explanatory Memorandum that the communication of copyright protected material via the homepage or website of a library will in many cases be in competition with commercial on-line deliveries of material since perfect quality copies of any work could be made available to a large number of users, whether on-site (with a multiplicity of screens in the library) or off-site (to other libraries or remote users)[68].

- Article 5(2) (d) exempts the ephemeral fixations made by broadcasting organizations by means of their own facilities and for their own broadcasts.

Article 5(3) provides Member State with the possibility of certain limitations both to the reproduction right and to the communication to the public right in the following cases :

- use of a work or other subject matter (such as a sound or visual recording) for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated, against fair remuneration to rightholders. In any case, only the part of the use which is

justified by its non-commercial purpose may be exempted from the exclusive right.

- uses to the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature and to the extent required by the specific disability (handicapped persons);

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

- quotations for purposes such as criticism or review, provided that they relate to a work or other subject matter which has already been lawfully made available to the public, that if possible, the source is indicated, and to the extent required by the specific purpose (quotations);

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

Technological measures

The proposal conveys an on-going concern of the Commission which consists of protecting technological measures, such as anti-copy devices or electronic copyright management systems, by preventing them from being circumvented[69].

According to Article 6 of the Directive, Member States shall provide adequate legal protection against on one hand the act of circumvention itself , and on the other hand, against the so-called preparatory activities, i.e. any act of commercial distribution or promotion of devices enabling the circumvention of technical measures. Therefore, any activities, including manufacture or distribution of devices of the provision of services, which (a) are promoted, advertised or marketed for the purpose of circumvention, or (b) have only limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating without authority the circumvention of any effective technological measure designed to protect any copyright or any rights related.

The 'technological measures' are defined as "*any device, product or component that, in the normal course of its operation, is designed to prevent or inhibit the infringement of any copyright or any rights related to copyright as provided by law or the sui generis right"*. Technological measures shall only be deemed to be 'effective' where the access to or use of a protected work or other subject matter is controlled through application of an access code or any other type of protection process which achieves the protection objectives in an operational and reliable manner with the authority of the rightholders. This requirement of effectiveness of the measure would imply that rightholders have a duty to demonstrate the effectiveness of the technology chosen in order to obtain protection.

The provision only covers the activities and services whose main commercially significant purpose or use is to circumvent, which would ensure that general-purpose electronic equipment or service is not prohibited even if they may be used to this end.

It is worth mentioning that along with the protection conferred by this proposal, another protection for the technical copyright protection mechanisms can be found in the directive on the protection of

conditional access services[70] which applies to conditional access systems to services normally offered against remuneration. Therefore , an encryption system protecting the access to an on-line entertainment service (on-line music or video) might be protected against illicit devices enabling its circumvention on the ground of both directives.

Rights Management Information

Article 7 of the proposal gives Member states appropriate flexibility in implementing adequate legal protection against any person performing without authority any of the following acts :

- to remove or alter any electronic rights management information

- to distribute, import for distribution, broadcast, communicate or make available to the public copies of works or other subject matter

This provision conveys the similar protection laid down by WIPO Treaties in order to protect any digital information, copyright notice or identification systems attached to protected works.

SECTION 14. PROTECTION OF DATABASES

One of the main reasons why US operators would establish themselves in the European Union is the protection granted to databases. Indeed, the EU has been the first to set up a coherent regulatory framework for protecting databases of information, whether they are original or not. This has been refused by US case law so far and is still discussed in the US Senate, in a very controversial way.

The recent European directive on the legal protection of the databases[71] provides a double protection for databases defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means[72]". First, they can be protected as such by the general rules on copyright if they constitute the author's own intellectual creation, by reason of the selection or arrangement of their content. Thus the standard of protection is defined at a European level[73].

Concerning the authorship of a database, the directives states:

"*The author of a database shall be the natural person or group of natural persons who created the base or, where the legislation of the Member States so permit, the legal person designated as the rightholder by that legislation[74]. Where collective works are recognized by the legislation of a Member State, the economic rights shall be owned by the person holding the copyright. In the case of a database created by a group of natural persons jointly, the exclusive rights shall be owned jointly.* "[75]

The duration of the right is the same as what is provided in the general rules of copyright, thus 70 years after the death of the author.

The non-original databases shall be protected by a sui generis right which prevents extraction and/or reutilization of the whole or of a substantial part of the contents of that database.

This new right vests upon the maker of a database, which is defined in recital 41 of the directive as "the person who takes the initiatives and the risk of investing". Consequently, the rightholder may be a natural person or a legal entity.

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

SECTION 15. LIABILITY OF ON-LINE INTERMEDIARIES

Liability for on-line intermediaries[76], such as access providers, hosting services or network operators, for infringements operated by others on the network, has always been a hot issue of the Information Society. Is an Internet access provider liable for child pornography images available on the Net ? Is a BBS operator liable for copyright infringements committed by the users of his system ? Is a hosting service liable for defamatory, criminal or counterfeiting material that is posted on his pages ? The issue is very delicate since it can be considered as the crossroads between the legitimacy of applying the law on the web, as in the physical world, and the freedom of expression and the practical impossibility of controlling the content which are claimed by many users and intermediaries as key features of the Information Society.

The European Commission has decide to rule this matter horizontally, i.e. by imposing the same rules of liability whatever the type of infringement is : copyright, defamation, illegal and harmful content, etc... It is interesting to note that the lines of this new regime are rather similar to the US Digital Millennium Copyright Act.

The Proposal makes a distinction between three types of situations. In each of these situations, conditions are laid down for limiting the liability of service providers. It is worthwhile noting that this limitation of liability does not prevent injunctive relief.

- ***Mere conduit*** : this situation consists in the transmission on a communication network of information provided by a person who places information on-line or the provision of access to a communication network. The Draft specifies in article 12 (2) that this includes also the automatic, intermediate and transient storage of the information if this takes place for the sole purpose of carrying out the transmission. In this case, the provider carrying out this conduit shall not be held liable on condition that :
  - he does not initiate the transmission,
  - he does not select the receiver of the transmission, and
  - he does not select and does not modify the information contained in the transmission.
- ***Caching*** : information stored in the intermediate and temporary cache made by a service provider would not imply his liability on condition that :
  - the provider does not modify the information,

- the provider complies with the conditions on access to the information;

- the provider complies with the rules regarding the updating of the information, specified in a manner consistent with industry standards,

- the provider does not interfere with technology used to obtain data on the use of the information; and

- the provider acts expeditiously to remove or to disable access to the information upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or that access to it has been disabled or that a competent authority has ordered such removal or disablement to take place.

- ***Hosting :*** the hosting service provider would not be held liable for illegal activity undertaken by an user of his service, if :

  - he does not have the actual knowledge that the activity is illegal and, as regards claims for damages, is not aware of facts or circumstances from which illegal activity is apparent, and

  - upon obtaining such knowledge or awareness, he acts expeditiously to remove or disable access to the information.

On this matter of liability, the European Commission strongly encourages industry self-regulatory systems, including the establishment of codes of conduct and hot line mechanisms.

CONCLUSION

Early development of the Internet and electronic commerce has challenged the law in an unprecedented way. Scholars and legislators have wondered how the regulation could fit the new electronic environment. It has also been questioned whether the existing legal framework will be able to cover the new applications offered by the technology.

The choice of the European Institutions has been in favor of a tailored regulation and it has proceeded in a case by case approach. So the law, in turn, challenges electronic commerce. We note that most of those texts are of minimum harmonization, which means that the transposition in the national framework can be different from country to country, which makes things less simple than it could appear at first sight.

Anyway, one of the central orientations of that way of acting is the protection of the weakest part in the transaction process : the consumer. But one can wonder if that policy will at the same time meet the needs of another important party which is the 'merchant'. A parallel question concerns the cost of consumer protection, because the implementation and the observation of all these rules require time and money. It is not sure whether the consumer indeed requires such great protection.

But it remains that some fields have to be regulated, mostly because they are common to a lot of different activities. One thinks of the regulation of electronic signatures, privacy or copyright. In those cases, the regulation is for the benefit of all actors of the Information Society. It allows business to enjoy a clearer regulatory framework in which it can operate.

June 1999

Séverine Dusollier,
Laetitia Rolin Jacquemyns
Researchers , CRID (Centre of Research in Computer and Law)
severine.dusollier@fundp.ac.be
laetitia.rolin@fundp.ac.be

[11] European Commission Communication (COM(97)157) of April16, 1997, "A European Initiative in electronic commerce) available at <http://www.cordis.lu/esprit/src/ecomcom.htm>

[2] M. BANGEMANN, "Which rule for the online world", Info., vol 1., n°1, feb. 1999, p. 11.

[3] see http://www.ispo.cec.be/infosoc/legreg/actionla.html

[4] see below

[5] see http://www.jura.uni-muenster.de/eclip/

[6] Other partners are the Professeur Herbert Burkert from the University of St-Gallen, who is also the President of the Legal Advisory Board by the European Commission , and a Belgian management company, the Bureau Van Dijk.

[7] European Council and Parliament Directive 98/34/EC, June 22, 1998, OJ L 204, 21.07.1998, as amended by the Directive 98/48/EC, July 20, 1998, OJ L 217, 05.08.1998, available at http://europa.eu.int/eur-lex/en/lif/dat/1998/en_398L0048.html

[8] article 1(2).

[9] European Parliament and Council Directive 97/7/EC of May 20, 1997, OJ L 144, 4.6.1997, available at http://europa.eu.int/comm/dg24/policy/developments/dist_sell/dist01_en.html

[10]. Council and European Parliament Directive 98/84/EC of November 20, 1998, OJ L320, 28.11.1998

[11] Council and European Parliament Directive 96/9/EC of March 11, 1996, OJ L77, 23.6.1996, available at http://www2.echo.lu/legal/en/ipr/database/database.html

[12] 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, OJ 23.11.1995 No L. 281 p. 31. http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html

[13] European Commission Proposal of October 14, 1998, available at http://europa.eu.int/comm/dg15/en/finances/consumer/891.htm

[14] European Commission Proposal of November 18, 1998, available at http://www.ispo.cec.be/Ecommerce/legal.htm#legal

[15] European Commission Proposal for a Directive amending Directive 77/780/EC on the coordination of laws, regulations and administrative provisions relating to the taking-up, the pursuit and the prudential supervision of the business of credit institutions of 29 July 1998.

[16] European Commission Proposal for a Directive on the taking-up, the pursuit and the prudential supervision of the business of electronic money institutions of 29 July 1998

[17] European Commission Proposal of May 13, 1998. available at http://www.europa.eu.int/comm/dg15/en/media/infso/com297en.pdf

[18] European Commission Proposal of December 10, 1997; revised proposal on May 21, 1999, available at http://europa.eu.int/comm/dg15/en/intprop/intprop/copy2.htm

[19] Information available at http://europa.eu.int/comm/dg15/en/finances/consumer/99-559.htm

[20] EEC Rome Convention on the law applicable to contractual obligations, [1980] OJ L226/1

[21] J. FAWCETT & P. TORREMANS, "Intellectual Property and Private International Law", Clarendon Press Oxford, 1998,

p. 579

[22] More exactly, the application of the national law of Member States having transposed it.

[23] C. de TERWANGNE & S. LOUVEAUX, Data protection and online networks, C.L.S.R., 08/1997, n° 13/4, pp. 234-246

[24] For a detailed and thorough analysis , see FAWCETT & TORREMANS, op.cit.

[25] J. GINSBURG, M. GAUTHIER,The celestial jukebox and earthbound courts : Judicial competence in the European Union and the United States over copyright infringements in cyberspace, R.I.D.A., 07/1997, n° 173, pp. 61-131.

[26] annex II of the Draft e-commerce directive

[27] Green Paper of December 3, 1997, followed by a Commission Communication of March 10, 1999, available at http://www.ispo.cec.be/iconvergencegp/

[28] R. PREISKEL, N. HIGHAM, Liberalization of telecommunication infrastructure and cable television networks. - The European Commission's Green Paper., Tel.Pol., 07/1995, n° 19/5.; see also Baker and McKenzie, EU developments in IP, IT and telecommunications law, C.L.S.R., different articles published in 1998 and 1999.

[29] A. SALAÜN, E-Commerce. = Consumer protection - Proposals for improving the protection of online consumers, C.L.S.R., 06/1999, n° 15/3, pp. 159-167

[30] available at http://europa.eu.int/comm/dg15/en/media/commcomm/commer.htm

[31] Directive 95/46/EC, op.cit.

[32] Defined as any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the conclusion of a contract between those parties (article 2.4). This clearly covers contracts entered into on an open network such as the Internet.

[33] Article 3 1.

[34] Article 4.

[35] Article 6 1. and 6.2..

[36]Article 7 1.

[37] h ttp://www.un.or.at/uncitral/english/sessions/wg_ec/wp-79.htm

[38] For an in-depth analysis of the contractual rules in the draft directive, R. JULIA BARCELO, "A new legal frameworks for electronic contracts ", CLSR vol 15, n°3, 1999, p.147-158.

[39] The explanatory memorandum of the Draft directive gives three examples of such formalities : the requirements as to the medium used for the contractual process (paper form, number of copies or printed contract), the requirements as to human presence, the requirements as to the involvement of third parties.

[40] We note that in the particular case of the electronic money instrument, the technology keeps changing, the

applications mentioned are the actual ones but could change.

[41] Commission recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, OJ, n° L 208, 02.08.97, p.52.

[42] Article 1.1 and 2 (a).

[43] For a complete list of the obligation see article 3 of the recommendation.

[44] Article 6 and 8.

[45] Commission proposal for directives on the regulation of the Commission proposal for European Parliament and Council Directives on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions. The only version available on the Internet is different than the actual version that is discussed in the European Parliament. It can be found at http://europa.eu.int/comm/dg15/en/finances/general/727.htm

[46] Article 1 (c).

[47] For more details on the indirect taxation of the electronic commerce see L; EDWARDS and C. WAELDE, "Law and the Internet, regulating cyberspace", Hart publishing, 1997, p.155-170.

[48] Sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member, States relating to turnover taxes Common system of value added tax: uniform basis of assessment.

[49] S. EDEN, “The Taxation of Electronic Commerce” , in Law and the Internet, Hart Publishing, Oxford, 1997, p.155.

[50] Idem.

[51] Value Added Tax Act 1994, Schedule 5.

[52] S. Eden, “The Taxation of Electronic Commerce”, in Law and the Internet, Hart Publishing, Oxford, 1997, p.156.

[53] UK VAT Order 1992 SI 1992/3121, Art. 16; Belgian Code on VAT, article 21§3,7°.

[54] see the example of the P3P (Privacy Preference Platform) developed by W3C, http://www.w3.org/Privacy/Activity.html

[55] op. cit, see note 11

[56] Directive 97/66/EC of the European Parliament and the Council of the 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24/1,

[57] Recital 26 of the Data protection directive.

[58] other exemptions are provided in the directive, but they are not relevant for electronic commerce environment.

[59] COM (95) 382 final of 19 July 1995

[60] Directive on the legal protection of computer programs, May 14, 1991, OJ L122, 17.5.1991; Directive on rental and lending rights and on certain neighbouring rights, November 19, 1992, OJ L346, 27.11.1992; Directive on satellite broadcasting and cable retransmission of September 27, 1993, OJ L248, 6.10.1993; Directive on the

harmonization of the term of protection of copyright and certain related rights of October 29, 1993, OJ L290, 24.11.1993; Directive on the legal protection of databases of 11 march 1996, OJ. 23/6/96; Follow-up of the Green Paper on copyright and related rights of 20/11/96; available at http://europa.eu.int/comm/dg15/en/intprop/intprop/index.htm.

[61] S. von LEWINSKI, A successful step towards copyright and related rights in the information age : The E.C. proposal

for a harmonization directive, E.I.P.R., 04/1998, n° 20/4, pp. 135-139

[62] WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty, http://www.wipo.int

[63] Follow-Up to the Green Paper on Copyright and Related Rights in the Information Society, 20.11.96, COM(96) 568 final, Chapter 2, p. 9

[64] Y. Gendreau, "Reproduction right and Internet", RIDA, January 1999, p. 3-81

[65] Recital 23 of the Directive

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

[66] Recital 18 of the Proposal

[67] M. HART, The proposed directive for copyright in the information society : Nice rights, shame about the

exceptions, E.I.P.R., 05/1998, n° 20/5, pp. 169-171

[68] Directive Background, op. Cit., p. 9

[69] S. DUSOLLIER, Electrifying the Fence : The legal protection of technological measures for protecting copyright, E.I.P.R., 06/1999, n° 21/6, pp. 285-297

[70] op.cit, see note 8

[71] op. cit. note 10

[72] Art. 1 (2) of the Database Directive

[73] A. STROWEL & J.P. TRIAILLE, Le droit d'auteur, du logiciel au multimédia : droit belge, droit européen, droit comparé, Story-Scientia, 1997, XXIV, 510 p.

[74] For instance, in the employer or the person who commissioned the work will be the author

[75] Art. 4 (1) of the Database Directive

[76] M. SCHAEFER, C. RASCH, T. BRAUN, Liability of on-line service and access providers for copyright infringing third-party contents, E.I.P.R., 04/1999, n° 21/4, pp. 208-211; R. JULIA-BARCELO, Liability for on-line intermediaries : An european perspective, E.I.P.R., 12/1998, n° 20/12, pp. 453-463