ALAI 2001 National Report
Session IC
France

ALAI Conference 2001 – NEW YORK – 13-17 June 2001

Regimes supplementary to and competing with copyright

Technical protection arrangements viewed in a broader context

Questionnaire

General Rapporteur: Séverine Dussolier

University Schools of Notre Dame de la Paix, Namur, Belgium

Gilles Vercken

Cabinet Gilles Vercken

An attorney of the Paris Bar

General preliminary remarks

Concerning the form of the questionnaire

The questionnaire consists of ten questions, only the last of which deals directly with copyright.

The questionnaire is very detailed and includes a very large number of questions.

Within the framework of French law, many questions overlap, particularly because the question subjects are either transverse, or particular. Responses to transverse questions sometimes constitute responses to the particular questions, and vice versa.

That is why certain responses are very succinct, or identical for several questions.

Concerning the basis of the questionnaire

Generally speaking, French positive law includes many provisions that could be used to protect acts of neutralisation of the protective arrangements for works outside protection by reservation mechanisms coming under copyright and neighbouring rights.

However, the purpose of those provisions is not to protect the works as such.

They make it possible to move against actions that have indirectly made it possible to obtain access to the said works by neutralisation of the systems.

These provisions are essentially as follows:

- computer criminal law, and essentially access to or fraudulent presence in an automated data system
- violation of private correspondence (article 226 – 15 of the CPI)
- article 79 – 1 ff. of the law of 30 September 1986 concerning fraudulent interception of televised programmes – of broad application since distribution by networks may be characterised as television broadcasting.

Moreover one of the important legal difficulties brought up by the multiplication of texts results from the coherence between various texts pursuing different objectives:
- freedom of telecommunications and users' rights
- protection of content by criminal law systems
- protection of content and exceptions in the common law of artistic and literary property
- specific exceptions to software law
- protection of private correspondence.

It then appears that all of the legal protection mechanisms come under other fields of law that can be applied in order to ensure protection of the technical measures and/or of the information relative to the protected objects.

However, this application is never aimed at providing protection of assignees. Hence it seems that this legal arsenal will be usefully supplemented by provisions enabling the holders of rights to have some specific legal tools proper to their interests, but without excluding application of the existing legal tools.

The latter point is an important one, since protection by mechanisms outside copyright has the advantage of not being subject to the limits that could result from application of the provisions of the draft directive concerning copyright and neighbouring rights, which provide for protection of the technical measures insofar as compatible with the benefit of the exceptions.

In view of the legal uncertainties concerning the exact relationship that is to be instituted between protection of the technical measures and the benefit of the exceptions, and pending discussion and debate at the time of transposition into French law of the directive once it is adopted, the traditional means of protection, and particularly criminal computer law, remain – and will remain – reliable tools available to practitioners.

Outline of the questionnaire:

1. **Acts of neutralisation**
2. **Common law of liability**
3. **Law relating to audio-visual, cable and satellite and protection of encrypted services or programmes, protection of conditional access services**
4. **Telecommunications law**
5. **Computer crimine**
6. **Commercial practise and unfair competition**
7. **Protection of the technical arrangements**
8. **Other types of protections**
9. **Exceptions, fundamental rights, interests of third parties and the public interest**
10. **Application of the types of protection contemplated in questions 1 to 9 to works protected by copyright**

* * * * * * * * * * *

1. Acts of neutralisation

Are the following acts forbidden in your country? By virtue of what legislation?

a. Access without authorisation to a computer system that is technically secured or has protected content.

These acts are outlawed by law n° 88- 19 of 5 January 1988 (Godfrain law), now incorporated into articles 323-1 ff. of he new Penal code:

"The act of accessing or of fraudulently remaining in all or part of a system for automatic data processing is punished by one year of imprisonment and by a fine of 100,000 F".

We must point out that French law does not make the protected nature or lack thereof of the system a condition for attacking the action (along those lines, Court of Appeals of Paris, 11th chamber, 5 April 1994, Court of Appeals of Toulouse, 3rd Chamber, 21 January 1999).

b. Receiving data or protected content without authorisation or without paying the required remuneration.

We should mention that the responses may vary in the light of what is understood by the term "protected content".

This may refer to technical protection, or to protection under intellectual property law.

If one accepts the latter meaning, the acts mentioned constitute an infringement of copyright or of the neighbouring rights (including the right sui generis held by the producer of a database), this under the conditions laid down in the text (exclusive monopoly and exceptions).

c. Access to technically secured computer system or to content protected by a false name or by a password.

These acts are forbidden by virtue of article 323-1 ff. of the new Penal Code, which apply to any penetration of a system.

"Fraudulent access, in the meaning of the law, refers to all irregular procedures for penetration of a system" (Court of Appeals of Paris, 11th Chamber, 5 April 1994).

d. Access to technically protected content by supplying false financial data.

The response is affirmative and is identical with the previous one (application of articles 323-1 ff. of the New Penal Code).

e. Access to a technically secured computer system or to protected content by using a false IP (Internet Protocol) address.

The response is affirmative, on the same basis as the one described above.

f. Decoding the encrypted content without authorisation.

The same articles again apply.

g. Exceeding the authorised number of users or access time.

Exceeding the number of users is tantamount to fraudulently remaining and/or the act of overrunning the authorised access time is still sanctioned under articles 323-1 ff. of the new Penal Code, which also condemn fraudulently remaining in an automated data processing system.

Such actions may also constitute acts of infringement, any "overrun" of the authorisation granted by an assignee being an infringement (L. 335-2 of the Code of Intellectual Property).

h. Exceeding the number of authorised copies or a technical measure preventing production of copies.

The response is the same as the previous one.

2. Common law of liability

a. Can the neutralisation of the technical measures be sanctioned on the basis of the common law of civil liability?

One may contemplate application of article 1382 of the Civil Code: *"Any action whatsoever on the part of a person that causes harm to others obliges the party by whose fault the action has occurred to pay compensation"*.

This text is generally applicable.

On what conditions?

Above all, for the fault to be constituted, there must have been violation of an obligation. Hence it is necessary to determine the said obligation. General obligations, such as the obligation to observe diligence, may possibly be applicable.

Three elements must be present: prejudice, a generating fact and a causal link between them.

The weakness of the mechanism instituted under article 1382 of the Civil Code is due to the fact that it is up to the victim to prove those elements.

What is the situation with production and distribution of systems making avoidance possible?

Here again article 1382 of the Civil Code may apply. However, one may think that in this situation, the causal link between prejudice and the fault will be hard to establish.

b. Have the Courts of Appeals and the Lower courts already sanctioned avoidance and/or marketing of equipment on the basis of civil liability? On what assumptions? How have they characterised the fault? Is an element of intent or of knowledge necessary? Does the fault consist in contributing to or in facilitating the violation of a right (copyright or other right)?

There are no precedents as far as we know relative to this problem. However, in the light of the precedents relative to application of article 1382 of the Civil Code generally, an element of intent or of knowledge would probably not be necessary (objective conception of personal action in French law).

c. In case neutralisation or distribution of equipment making neutralisation possible can be the object of proceedings on the basis of civil liability, on what assumptions could one escape such liability?

The only hypothesis making it possible to escape the liability provided for under article 1382 of the Civil Code is force majeure.

d. Could the fact of blocking access to data or to other objects that are technically protected constitute a misuse of law in your country?

The notion of misuse of law is a very subjective one in French law. Hence it is difficult to predict the decisions that would be made by the courts. But having said this, there is nothing against the notion, a priori, that the conclusion would be a misuse of law in the case mentioned.

3. <u>Law relating to the audio-visual sector, cable and satellite, and protection of encrypted services or programmes, protection of conditional access services</u>

a. Are encrypted programmes and/or services (for instance, pay television services, etc.) the object of regulation? Is that regulation found in civil, penal, administrative or public law? What is the objective of such provisions?

Encrypted programmes are regulated by law n° 86- 1067 of 30 September 1986, as modified by law n° 92- 1336 of 16 December 1992. That regulation is found in penal law.

Its objective was originally to protect the CANAL + Television channel against reproduction of its decoders.

b. Are decoding or reception of encrypted programmes and/or services without authorisation prohibited? Under what conditions? What is the objective of these regulations? What types of programmes and/or services are targeted? Must they be paying in order to benefit from protection?

The programmes targeted are "*televised programmes when the said programmes are reserved for a given public that accesses them by means of remuneration paid to the service operator"* (article 79-1 of the law). Hence there must be payment for the programmes.

Moreover the conditions are specific to this text.

Thus the Cour de Cassation (Supreme Court of Appeals) has recalled that installation in a public place (in the case in question, in the bar of a hotel) of a decoder did not constitute the violation targeted by article 79-3. (Cour de Cassation – Crim, 21 November 2000 – quoted by Lamy Droit des Médias et de la Communication – Actualités – n° 11 – 23 February 2001).

Hence use for purposes other than private ones is not one of the material criteria concerning the violation. It therefore seems clear that this text has its own logic, and that the conditions provided for in the texts relative to copyright in public use subject to the monopoly and private use covered by an exception are not applicable.

Who may file suit? What sanctions are provided for?

An action may be filed by the service operator.
The sanctions that are provided for are a fine and imprisonment (article 79-1 ff. of the law).

c. Does the prohibition also concern decoding or neutralisation equipment?

The prohibition also relates to those elements.

What are the prohibited activities?

Article 79-1 prohibits "*manufacture, importing with a view to sale or rental, offering for sale, holding with a view to sale, sale or installation of equipment, materials, systems or instruments designed, in total or in part, to fraudulently receive televised programmes, when the said programmes are reserved to a given public that accesses them by means of remuneration paid to the service operator"*.

Article 79-2 prohibits *"the action of ordering, designing, organising or disseminating advertising that, directly or indirectly, promotes an equipment item, materials, systems or instruments mentioned in article 79-1"*.

Does the law also prohibit non-commercial activities relative to such equipment items?

The answer is yes.
Article 79-3 prohibits *"organisation, defrauding the service operator of its rights, of reception by third parties of the programmes mentioned in article 79-1"*.
Article 79-4 sanctions *"the acquisition or holding, with a view to use of an equipment item, materials, systems or instruments mentioned in article 79-1"*.

With respect to decoding equipment, how does one define the unlawfulness of such systems?

The definition of unlawfulness of such systems seems to be teleological, since the law mentions equipment that is *"designed, in total or in part, to fraudulently receive"* the programmes in question.

The notion of "fraud" is a broad one.

How does the law [deal] with mixed systems, i.e., devices that have both a function, a legitimate use, and a function of illicit neutralisation? Who can file an action on the basis of the said law? What types of actions and of sanctions are provided for?

d. Are there circumstances under which decoding is authorised for the user? How do the precedents apply these rules and regulations?

e. Do you consider that these rules and regulations are adequate and effective?

The law does not deal with mixed systems. Hence the protection is identical. No circumstances can justify access and fraudulent maintenance.

The regulations under computer criminal law are particularly effective in ensuring protection of the technical measures.

f. Rules and regulations relative to conditional access:

A 1997 European directive protects conditional access services, namely, services access to which is subordinate to certain conditions, particularly to payment of remuneration, and sanctions the marketing of mechanisms facilitating neutralisation of conditional access systems. The protected services are radio and television, as well as the information society services, the examples mentioned in this connection being, in particular, services relating to video on request, on-line access to a database, on-line publication and other services supplied on the networks.

1. Does similar protection exist in your country? In what legal field (audio-visual law, specific law)?

2. In case the answer is yes, what is the objective of that legislation? What types of services are targeted? What are the protection conditions? Is conditional access defined by the remuneration criterion? Does the law prohibit the act of neutralising the technical measure relating to access or the devices allowing such neutralisation? In the latter case, what activities are forbidden (sale, manufacture, possession, provision of services, etc…)?

3. The European directive explicitly includes information society services in its fields of application, which moreover are defined as services provided remotely in response to an individual request by the addressee of the service. Does your legislation concerning conditional access also cover information society services? In other words, can it be applied to the services supplied on the Internet or on other electronic services?

The law of 1 August 2000 relative to freedom of communication lays down the regime applicable to operators of conditional access systems (article 95 of the law). However, the main purpose of those texts is to settle the conditions under which the said operators have to allow access to such technologies without distortion of competition.

Outside of the texts already mentioned (protection by computer criminal law – protection of decoders), there are no specific arrangements.

4. Telecommunications law

We must remind you that telecommunications law is based on a few major principles that define users' rights.
To present them, we will use the classification made by Professor Michel Vivant (LAMY: DROIT DE L'INFORMATIQUE ET DES RESEAUX, Edition 2000, n° 1944):

1. The right to network connection
2. The right to correspondence secrecy
3. The right to operator neutrality
4. The right to recourse against the suppliers
5. The right to protection against improper clauses.

We also remind you of the existence of the above-mentioned law of 30 September 1986, modified by the law of 16 December 1992, that sanctions unauthorised access to a television when the said access is conditional on payment of a remuneration to the service operator.

a. The rules and regulations relative to telecommunications may sanction unauthorised interception of communication, either by decoding or by any other act providing access to the content at the time of its transmission on a telecommunications network. This type of provision could constitute the basis for an action against decoding or unauthorised access to data transmitted on telecommunications networks. Does the law on telecommunications contain any such prohibition?

The answer is yes. Such a prohibition is stipulated by law n° 91-646 of 10 July 1991 relative to secrecy of correspondence transmitted by way of telecommunications.

1. What is the act in question? Does the law refer to equipment allowing or facilitating such interception?

Article 226-15 of the Penal Code sanctions "*the act, committed in bad faith, of intercepting, diverting, using or disclosing correspondence that is issued, transmitted or received by way of telecommunications"*.
The law mentions equipment, since the said article 226-15 also represses the act, committed in bad faith, of *"proceeding with installation of devices designed to make such interceptions"*.

2. Must the content be encrypted or otherwise protected to benefit from protection?

The answer is no. Correspondence of all types is protected.

3. Is the prohibition on interception or distribution of equipment allowing interception subject to certain exceptions (for instance, when the decoding or interception devices meet certain technical standards)?

No, application of the text is not subject to technical criteria.

4. Who may file an action on the basis of these provisions? What actions and sanctions are provided for?

Persons whose correspondence has been intercepted, diverted, used or disclosed in bad faith. Article 226-15 of the Penal code provides a penalty of one year of imprisonment and a fine of 300,000 F.

b. Telecommunications law may also impose observance of certain technical standards on terminal devices. This could constitute a way of prohibiting telecommunications systems allowing unauthorised reception of communications. What is the situation in this respect in your legislation?

A text requires terminal devices to observe certain technical standards. We are referring to decree n° 92-116 of 4 February 1992 relative to approval of telecommunications terminal equipment, to its connection conditions and to authorisation of installers (LAMY: DROIT DE L'INFORMATIQUE ET DES RESEAUX, Edition 2000, n° 1939). But these texts are not connected with protection of the content.

5. Computer crime

a. Does your country have legislation concerning computer crime?

The answer is yes. Law n° 88-19 of 5 January 1988, known as the "Godfrain law", now incorporated into articles 323-1 ff. of the new Penal Code (cf. responses to the previous questions).

Do avoidance of technical protection or unauthorised access to a computer system or network constitute an offence?

The answer is yes.
Article 323-1 of the new Penal code provides that "*the act of accessing or of maintaining oneself, fraudulently, in all or part of an automated data processing system is punished by imprisonment of one year and by a fine of 100,000 F".*

What is the objective of making such actions criminal acts?

To sanction a new type of crime against which recourse to the common law lacked effectiveness, particularly because of the principle of speciality in criminal law.

b. How are the acts that are prohibited defined? Is the way unauthorised access is made possible specified, for instance, supply of a false password, decoding, or some other act of piracy?

The forbidden acts are defined broadly. The way access is made possible is not specified. The fact is that it is the mere act of fraudulently accessing a system for automated data processing that is made criminal, the means used for that purpose being unimportant.

c. Is the criminal law also aimed at equipment making commission of such offences possible (sometimes called "hacker tools")? Failing this, could the seller or the manufacturer of such equipment be prosecuted as accomplices? What are the penalties provided for such offences?

Criminal law is not directly aimed at the equipment items.
The seller or the manufacturer of such equipment items and/or any person could be prosecuted on the basis of the general texts relative to complicity.

The fact is that article 121-7 of the Penal code provides that *"a person is an accomplice in a crime or an offence if he knowingly, by aid or assistance, has facilitated preparation or consummation thereof".*

d. What are the elements of the offence? Is a fraudulent intent or some other moral element required?

A material element and a moral element are necessary for the infraction to occur. The material element consists in access to and/or unauthorised maintenance in a system. The moral element lies in the knowledge of an absence of a right to access and/or to maintain oneself in the system.

e. Have the courts already applied these provisions in the context of a technical protection measure or of unauthorised access to data or to other technically protected objects?

The answer is yes. However, the application of the texts does not depend on the existence of limited access or access subject to conditions. Thus mere access and/or maintenance, as long as it is not explicitly authorised, is sanctioned (Court of Appeals of Paris – 5 April 1994).

f. In the absence of a law of computer crime, could certain traditional offences (theft, fraud, forgery, break-in, etc.) be used to characterise unauthorised access and/or neutralisation of a technical system? Are there cases in the precedents?

In principle such charges could apply to access to or unauthorised maintenance in a computer system or in a network as long as entry is under the conditions laid down in the text.

6. Commercial practise and unfair competition

a. In your country, has the marketing of decoding devices or equipment or of decoders been sanctioned, in the absence of specific protection, on the basis of the law concerning unfair competition? Under what conditions?

There are no cases of jurisprudential application of the law concerning unfair competition to marketing of decoding devices or equipment in French law.

b. What are advantages, drawbacks or limits of application of the law concerning unfair competition to such practises? Do you think such protection is effective and efficient?

The purpose of the law concerning unfair competition and of law regarding parasitical actions is different. This law is based on a broad application of article 1382, relative to civil liability.

The drawbacks lie in the difficulty of proving elements making it possible to act on this basis, and particularly the existence of a fault in the absence of private rights to the object of protection.

This protection cannot be effective, since it depends on the circumstances in each case, and hence does not provide sufficient predictability.

In addition one must have a dilution of the forms of specific legal protection by an inappropriate extension of protection by unfair competition or parasitical actions.

7. Protection of the technical arrangements

The technical protective arrangements themselves may be the object of private law. It may be a question of a copyright or of a patent to the software, or else of manufacturing secrets or of business secrecy protecting the decoding key or the technical mechanism itself. Getting around the software or the technical means or manufacturing or distributing avoidance equipment could constitute an act of reproduction (decompilation of the software, for instance), of unauthorised exploitation or a disclosure of manufacturing secrets or business secrets.

a. Is your legislation concerning copyrights, patents or business secrecy applicable in this context? Under what conditions? Have the precedents already protected a technical mechanism by way of this approach?

The legislation relative to software can perfectly well apply, as long as the technical system uses software.

This protection is now provided in positive law by copyright, and it cannot be provided by patents, whatever the status of the present debate concerning patentability of software may be.

Furthermore the code of Intellectual Property henceforth protects technical systems for protection of software by means of a specific text (it being recalled that computer criminal law may also apply).

Article L 122 – 6 – 2 of the CPI provides as follows:

"**Art. L. 122-6-2** (Law n° 94-361 of 10 May 1994). Any publicity or use notice relative to the means of doing away with or neutralising any technical arrangements protecting a software item must mention the fact that the illicit use of such means is subject to the sanctions provided for in case of infringement. A decree in Council of State will lay down the conditions for application of the present article."

The decree has not yet been adopted, and there are no precedents with respect to application of this text.

Moreover the protection relative to manufacturing secrets and know-how may apply.

But these protective systems are governed by specific conditions, that will sanction actions having made it possible to obtain access to information relative to the protective system, and not to the attack relative to the protective system itself.

b. What are the exceptions to these specific protective regimes from which a person who has gotten around the protection or has made/distributed avoidance systems could benefit?

There is an exception relative to the interoperability of the software (article L. 122-6-2 of the Code of Intellectual Property).

The said article provides as follows:

"**Art. L. 122-6-1** (law n° 94-361 of 10 May 1994). I. – The acts provided for in points 1 and 2 of article L. 122-6 are not subject to the author's authorisation when they are necessary to allow use of the software in accordance with its purpose by the person having the right to use it, including the right to correct errors.
However, the author is entitled to reserve, by contract, the right to correct the errors and to determine the special procedures to which the acts will be subject that are provided for in points 1 and 2 of article L. 122-6 necessary to allow use of the software in accordance with its purpose by the person having the right to use it.

II.- The person entitled to use the software may make a back-up copy when this is necessary to preserve use of the software.

III.- The person entitled to use the software may, without the author's authorisation, observe, study or test the operation of the said software in order to determine the ideas and principles underlying any element whatsoever of the software when he carried out any operation relating to loading, display, execution, transmission or storage of the software that he is entitled to carry out.

IV.- The reproduction of the software code or the translation of the form of the said code is not subject to the author's authorisation when the reproduction or the translation of the form in the meaning of point 1 or of point 2 of article L. 122-6 is indispensable in order to obtain the information required for the interoperability of a software item created independently with other software items, as long as the following conditions are met:

1. The said acts are carried out by the person entitled to use a copy of the software or in his behalf by a person authorised for that purpose.

2. The information needed for interoperability has not been made easily and quickly accessible to the persons mentioned in point 1 above.

3. And the said acts are limited to the parts of the original software necessary for the said interoperability.

The information obtained in this way may not be:

1. Used for purposes other than realisation of the interoperability of the software created in an independent way.

2. Or communicated to third parties unless that is necessary to the interoperability of the software created independently.

3. Or used for the development, production or marketing of a software item the expression of which is substantially similar or for any other act constituting an attack on the copyright.

V.- The present article may not be interpreted as allowing a person to attack the normal exploitation of the software or to cause unjustified prejudice to the author's legitimate interests.
Any stipulation contrary to the provisions laid down in points II, III and IV of the present article is null and void."

Within the framework of this exception, it would be possible to attack the technical protection systems based on a software item to adapt the latter to another compatible software item and/or to compatible hardware (Court of Appeals of Paris, 12 December 1997 – interoperability for adaptation of the ZIP floppy disk software to a reader).

We should also point out that the French courts have given a very restrictive interpretation of the back-up copy. It may be made only if the software publisher has not provided it, and if it is useful.

8. Other types of protection

a. How could one protect the technical measures outside of legislation or the legal mechanisms mentioned above? By what type of legislation or legal mechanisms (for instance, law concerning protection of personal data and private life, property right, etc…)? On what assumptions?

b. In particular, do you think that the law of contracts can offer an effective solution to prohibit neutralisation of technical protection?

1. **Assumption of a contract managed by the technical measure itself (case of on-line licenses) that would prevent neutralisation. Is such a contract valid?**

Such a contract would be valid "a priori". However, such a contract could not prohibit decompilation for interoperability purposes.

Moreover the contracts proposed by the authors' companies provide that an authorisation granted in connection with rights is valid only subject to the use of certain software items, the said software items not allowing downloading, but only streaming.

2. **Assumption of a contract concluded with the computer or electronics industry that would force them to develop devices respecting the technical measure or not neutralising it? Have such negotiations taken place in your country?**

We have no knowledge of negotiations along those lines, but that does not mean that they do not exist.

9. Exceptions, fundamental rights, interests of third parties and the public interest

a. Are there general limitations on the types of protection contemplated in this report, limitations that would apply independently of the legal provisions on which the action against neutralisation of technical measures is based (limitation resulting, for instance, from freedom of expression, freedom of information, the public interest, consumer protection, misuse of law, etc…)?
b. What is the position in your country of the computer and electronics industry? Are there products likely to be forbidden on the basis of the types of legislation mentioned above? How have their interests been taken into account?

We must remind you here of the fundamental rights of users we have previously mentioned:

1. the right to connection to the network
2. the right to secrecy of correspondence
3. the right to operator neutrality
4. the right to recourse against suppliers
5. the right to protection against improper clauses.

However, it is clear that new divergent interests will have to be taken into account in connection with discussion regarding transposition of the directive concerning copyright and neighbouring rights in the information society.

10. <u>Application of the types of protection contemplated in questions 1 to 9 to works protected by copyright</u>

a. Could the holders of rights make use of the legal mechanisms and provisions mentioned above either to prohibit neutralisation of the technical measures protecting their works, or to prohibit distribution of equipment making such avoidance possible or facilitating it? What protective arrangements could apply?

b. Are these various types of protection such as to be used alternatively to or jointly with specific protection of the technical measurements in connection with copyright?

c. What are the advantages and the drawbacks for the author of using these various legal provisions? Do these various legal regimes throw another light on the opportuneness of new and specific protection in the copyright field?

d. If the author can use such protection outside the copyright, could that justify carrying out the transposition of the provisions of the treaties of the World Intellectual Property Organisation in this field into legislation other than copyright legislation? Do you think this solution would be opportune and effective? If not, what are the failures and shortcomings of these existing provisions that could be remedied by specific protection in the copyright field?

Do you have any other remarks?

The holders of rights may now potentially call on all of the legal provisions recalled in the responses to the questionnaire.

However, it would seem better for them to have their own rules regarding protection of the technical measures. That will be the case within the framework of transposition of the directive concerning copyright and neighbouring rights in the information society.

Three minimum conditions would have to be met to ensure protection of the technical measures:

1- One of the important conditions is that this protection should be granted to the holders of rights, and not to any person involved in the chain of dissemination of the protected objects. It will then be up to the holders of rights to decide on the way in which they want to make use of their prerogatives, particularly by contract.

2- A second condition will have to be to ensure the effectiveness of the specific legal protection of the technical measures by avoiding a situation in which the beneficiaries of the exceptions could claim a right to such exceptions that would neutralise protection of the technical measures.

3- Finally, it is essential that the specific regimes for protection of the technical measures not prevent the holders of rights from using the other legal tools available to them in the present state of positive law.

ALAI 2001 Rapports Nationaux
Séance IC
France

Congrès de l'ALAI 2001 – NEW YORK – 13 – 17 juin 2001

Régimes complémentaires et concurrentiels au droit d'auteur

Les protections techniques vues dans un contexte plus large

Questionnaire

Rapporteur générale : Séverine Dussolier

Facultés Niversitaires Notre Dame de la Paix, Namur, Belgique

Gilles Vercken

Cabinet Gilles Vercken

Avocat au Barreau de Paris

Remarques préliminaires générales

Sur la forme du questionnaire

Le questionnaire est composé de dix questions, dont seule la dernière a pour objet direct le droit d'auteur.

Le questionnaire est très détaillé et comporte de très nombreuses questions.

Dans le cadre du droit français, beaucoup de questions se recoupent, notamment du fait que les thèmes des questions sont soit transversaux, soit particuliers. Des réponses aux questions transversales constituent parfois des réponses aux questions particulières, et inversement.

C'est la raison pour laquelle certaines réponses sont très succinctes, ou identiques pour plusieurs questions.

Sur le fond du questionnaire

D'une manière globale, le droit positif français comporte de nombreuses dispositions pouvant être utilisées pour protéger les actes de neutralisation des dispositifs de protection des œuvres en dehors de la protection par les mécanismes de réservation relevant du droit d'auteur et des droits voisins.

Toutefois, ces dispositions n'ont pas pour but de protéger les œuvres en tant que telles.

Elles permettent d'agir contre des agissements ayant permis indirectement d'avoir accès à ces œuvres par la neutralisation des systèmes.

Ces dispositions sont essentiellement les suivantes :

- le droit pénal de l'informatique, et essentiellement l'accès ou le maintien frauduleux dans un système automatisé de données
- l'atteinte aux correspondances privées (article 226 – 15 du CPI)
- l'article 79 – 1 et suivants de la loi du 30 septembre 1986, sur la captation frauduleuse de programmes télédiffusés – d'application large dés lors que les diffusions par réseaux peuvent être qualifiées de télédiffusion.

Par ailleurs, une des difficultés juridiques importantes posée par la multiplication des textes résulte de la cohérence entre différents textes poursuivant des objectifs différents :
- liberté des télécommunications et droits des utilisateurs
- protection des contenus par les systèmes de droit pénal
- protection des contenus et exceptions dans le droit commun de la propriété artistique et littéraire
- exceptions spécifiques au droit du logiciel
- protection des correspondances privées.

Il apparaît alors que l'ensemble des mécanismes juridiques de protection relevant d'autres domaines du droit peuvent être mis en œuvre pour assurer la protection des mesures techniques et/ou des informations relatives aux objets protégés.

Toutefois, cette mise en œuvre n'a jamais pour objectif d'assurer la protection des ayants droits. Il semble donc que cet arsenal juridique sera utilement complété par des dispositions permettant aux titulaires de droits de disposer d'outils juridiques spécifiques et propres à leurs intérêts, sans exclure pour autant l'application des outils juridiques existants.

Ce dernier point est important, car la protection par des mécanismes en dehors du droit d'auteur présente l'avantage de ne pas être soumise aux limites qui pourraient résulter de l'application des dispositions du projet de directive sur les droits d'auteurs et les droits voisins, qui prévoient la protection des mesures techniques dans la mesure compatible avec le bénéfice des exceptions.

Compte tenu des incertitudes juridiques sur la relation exacte devant être instituée entre protection des mesures techniques et bénéfice des exceptions, et dans l'attente des discussions et débats lors de la transposition en droit français de la directive une fois adoptée, les moyens classiques de protection, et notamment le droit pénal de l'informatique, demeurent – et demeureront – des outils fiables à la disposition des praticiens.

Plan du questionnaire :

1. **Actes de neutralisation**

2. **Droit commun de la responsabilité**

3. **Droit de l'audiovisuel, du câble et satellite et protection des services ou programmes cryptés, protection des services à accès conditionnels.**

4. **Droit des télécommunications**

5. **Criminalité informatique**

6. **Pratique commerciale et concurrence déloyale**

7. **Protection du dispositif technique**

8. **Autres protections**

9. **Exceptions, droits fondamentaux, intérêts des tiers et intérêt public**

10. **Application des protections envisagées aux questions 1 à 9 aux œuvres protégées par un droit d'auteur**

* * * * * * * * * * *

1 . Actes de neutralisation

Les actes suivants sont-ils interdits dans votre pays ? En vertu de quelle législation ?

a. Accéder, sans autorisation, à un système informatique techniquement sécurisé ou à du contenu protégé ?

Ces actes sont incriminés par la loi n° 88-19 du 5 janvier 1988 (loi Godfrain) aujourd'hui reprise dans les articles 323-1 et suivants du nouveau Code Pénal :

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende ».

Il faut noter que le droit français ne fait pas du caractère protégé ou non du système une condition de l'incrimination (en ce sens, *Cour d'Appel de Paris, 11° ch., 5 avr.1994*, *Cour d'Appel de Toulouse, 3° ch., 21 janv.1999*).

b. Recevoir des données ou du contenu protégé, sans autorisation ou sans s'acquitter de la rémunération prévue ?

Il convient de signaler que les réponses peuvent varier en fonction de ce que l'on entend par « contenu protégé ».

Il peut s'agir soit d'une protection technique, soit d'une protection au titre du droit de propriété intellectuelle.

Si l'on retient cette dernière acception les actes mentionnés constituent une contrefaçon, au titre du droit d'auteur ou des droits voisins (y compris le droit sui generis du producteur de base de données) et ce dans les conditions fixées dans les textes (monopole exclusif et exceptions).

c. Accéder à un système informatique techniquement sécurisé ou à du contenu protégé par le biais d'un faux nom ou d'un mot de passe ?

Ces actes sont interdits en vertu des articles 323-1 et suivants du nouveau Code Pénal qui s'appliquent à toute pénétration dans un système.

« L'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système » (*CA Paris, 11° ch., 5 avr.1994*).

d. Accéder à du contenu techniquement protégé en fournissant de fausses données financières ?

La réponse est affirmative et identique à la précédente (application des articles 323-1 et suivants du Nouveau Code pénal).

e. Accéder à un système informatique techniquement sécurisé ou à du contenu protégé en usant d'une fausse adresse IP (Internet Protocol) ?

La réponse est affirmative, sur les mêmes fondements que ceux décrits ci-dessus.

f. Décrypter du contenu crypté sans autorisation ?

Les mêmes articles s'appliquent encore.

g. Outrepasser le nombre d'utilisateurs ou le temps d'accès autorisés ?

Outrepasser le nombre d'utilisateurs équivaut à un maintien frauduleux et/ou le fait de dépasser le temps d'accès autorisé est sanctionné toujours par les articles 323-1 et suivants du nouveau Code Pénal qui condamnent aussi le « maintien » frauduleux dans un système de traitement automatisé de données.

Ces agissements peuvent également constituer des actes de contrefaçon, tout « dépassement » de l'autorisation consentie par un ayant droit étant une contrefaçon (L. 335-2 du Code de la propriété intellectuelle).

h. Outrepasser le nombre de copies autorisées ou une mesure technique empêchant la réalisation de copies ?

La réponse est identique à la précédente.

2. <u>Droit commun de la responsabilité</u>

a. La neutralisation des mesures techniques est-elle susceptible d'être sanctionnée sur la base du droit commun de la responsabilité civile ?

On peut envisager l'application de l'article 1382 du Code Civil : *« Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer »*.

Ce texte est d'application générale.

A quelles conditions ?

Avant tout, pour que la faute soit constituée, il faut qu'il y ait violation d'une obligation. Il est donc nécessaire de déterminer cette obligation. Des obligations générales, telles que l'obligation de diligence, peuvent éventuellement être applicables.

Trois éléments doivent être réunis : un préjudice, un fait générateur et un lien de causalité entre ceux-ci.

La faiblesse du mécanisme institué par l'article 1382 du Code Civil vient du fait qu'il appartient à la victime de prouver ces éléments.

Qu'en est-il de la fabrication et de la distribution des dispositifs permettant le contournement ?

Ici aussi l'article 1382 du Code civil peut s'appliquer. Cependant, on peut penser que dans cette situation le lien de causalité entre le préjudice et la faute sera difficile à établir.

b. Les cours et tribunaux ont-ils déjà sanctionné le contournement et/ou la commercialisation d'équipements sur la base de la responsabilité civile ? Dans quelles hypothèses ? Comment ont-ils caractérisé la faute ? Un élément d'intention ou de connaissance est-il nécessaire ? La faute consiste-t-elle à contribuer ou à faciliter la violation d'un droit (droit d'auteur ou autre) ?

Il n'existe aucun cas de jurisprudence relatif à ce problème à notre connaissance. Cependant, au regard de la jurisprudence relative à l'application de l'article 1382 du Code civil en général, un élément d'intention ou de connaissance ne serait probablement pas nécessaire (conception objective du fait personnel en droit français).

c. Dans le cas où la neutralisation ou la distribution d'équipements la permettant peuvent être poursuivis sur la base de la responsabilité civile, dans quelles hypothèses pourrait-on échapper à cette responsabilité ?

La seule hypothèse permettant d'échapper à la responsabilité prévue par l'article 1382 du Code civil est la force majeure.

d. Le fait de bloquer l'accès à des données ou à d'autres objets techniquement protégés pourrait-il constituer un abus de droit dans votre pays ?

La notion d'abus de droit présente un caractère très subjectif en droit français. Il est donc difficile de prédire les jugements des tribunaux. Ceci dit, rien ne s'oppose à priori à ce que l'on retienne l'abus de droit dans le cas visé.

3. <u>Droit de l'audiovisuel, du câble et satellite et protection des services ou programmes cryptés, protection des services à accès conditionnels.</u>

a. Les programmes et/ou services cryptés (par exemple les services de télévision payant, etc.) font-ils l'objet d'une réglementation ? Cette réglementation se trouve-t-elle dans le droit civil, pénal, administratif, public ? Quel est l'objectif de ces dispositions ?

Les programmes cryptés sont réglementés par la loi n° 86-1067 du 30 septembre 1986 modifiée par la loi n° 92-1336 du 16 décembre 1992. Cette réglementation se trouve dans le droit pénal.
Son objectif était à l'origine de protéger CANAL + contre la reproduction de ses décodeurs.

b. Le décryptage ou la réception de programmes et/ou services cryptés sans autorisation sont-ils interdits ? Dans quelles conditions ? Quel est l'objectif de cette réglementation ? Quels types de programmes et/ou services sont visés ? Doivent-ils être payants pour bénéficier de la protection ?

Les programmes visés sont les *« programmes télédiffusés, lorsque ces programmes sont réservés à un public déterminé qui y accède moyennant une rémunération versée à l'exploitant du service »* (article 79-1 de la loi). Les programmes doivent donc être payants.

Par ailleurs, les conditions sont spécifiques à ce texte.

La Cour de Cassation a ainsi rappeler que l'installation dans un lieu public (en l'espèce le bar d'un hôtel), d'un décodeur ne constituait pas l'infraction visée par l'article 79 – 3. (Cour de Cassation – Crim ; 21 novembre 2000 – cité par Lamy Droit des Médias et de la communication – Actualités – n° 11 – 23 février 2001).
L'usage à des fins autres que privées n'est donc pas un des critères matériels de l'infraction. Il semble donc clair que ce texte a une logique propre, et que les conditions prévues par les textes relatives au droit d'auteur en usage public soumis au monopole et usage privé couvert par une exception ne sont pas applicables.

Qui peut intenter une action ? Quelles sanctions sont prévues ?

Une action peut être intentée par l'exploitant du service.
Les sanctions prévues sont des peines d'amende et d'emprisonnement (article 79-1 et suivants de la loi).

c. L'interdiction concerne-t-elle également les équipements de décryptage ou de neutralisation ?

L'interdiction concerne également ces éléments.

Quelles sont les activités prohibées ?

L'article 79-1 prohibe *« la fabrication, l'importation en vue de la vente ou de la location, l'offre à la vente, la détention en vue de la vente, la vente ou l'installation d'un équipement, matériel, dispositif ou instrument conçu, en tout ou partie, pour capter frauduleusement des programmes télédiffusés, lorsque ces programmes sont réservés à un public déterminé qui y accède moyennant une rémunération versée à l'exploitant du service »*.
L'article 79-2 prohibe *« le fait de commander, de concevoir, d'organiser ou de diffuser une publicité faisant directement ou indirectement, la promotion d'un équipement, matériel, dispositif ou instrument mentionné à l'article 79-1 »*.

La loi interdit-elle aussi les activités non commerciales relatives à ces équipements ?

La réponse est affirmative.
L'article 79-3 réprime *« l'organisation, en fraude des droits de l'exploitant du service, de la réception par des tiers des programmes mentionnés à l'article 79-1 »*.
L'article 79-4 sanctionne *« l'acquisition ou la détention, en vue de son utilisation, d'un équipement, matériel, dispositif ou instrument mentionné à l'article 79-1 »*.

En matière d'équipements de décryptage, comment définit-on l'illicéité de ces dispositifs ?

La définition de l'illicéité de ces dispositifs semble être téléologique puisque la loi évoque un équipement *« conçu, en tout ou partie, pour capter frauduleusement »* les programmes visés.

La notion de « fraude » est large.

Comment la loi traite-t-elle les dispositifs mixtes, c'est-à-dire les appareils qui ont à la fois une fonction, une utilisation légitime et une fonction de neutralisation illicite ? Qui peut intenter une action sur la base de cette loi ? Quels types d'actions et de sanctions sont prévues ?

d. Existe-t-il des circonstances dans lesquelles le décryptage est autorisé pour l'utilisateur ? Comment la jurisprudence applique-t-elle cette réglementation ?

e. Estimez-vous que cette réglementation est adéquate et effective ?

La loi ne traite pas des dispositifs mixtes. La protection est donc identique. Aucune circonstance ne peut justifier l'accès et le maintien frauduleux.

La réglementation du droit pénal de l'informatique est particulièrement efficace pour assurer la protection des mesures techniques.

f. Réglementations relatives à l'accès conditionnel :

Une Directive européenne de 1997 protège les services d'accès conditionnel, soit les services dont l'accès est subordonné à certaines conditions, notamment au paiement d'une rémunération, et sanctionne la commercialisation de mécanismes facilitant la neutralisation des systèmes d'accès conditionnel. Les services protégés sont la radio et la télévision, ainsi que les services de la société de l'information, les exemples cités à cet égard étant notamment les services de vidéo à la demande, l'accès en ligne à une base de données, la publication en ligne et d'autres services fournis sur les réseaux.

1. Une protection similaire existe-t-elle dans votre pays ? Dans quel domaine juridique (droit de l'audiovisuel, loi spécifique) ?

2. En cas de réponse affirmative, quel est l'objectif de cette législation ? Quels types de services sont visés ? Quelles sont les conditions de la protection ? L'accès conditionnel est-il défini par le critère de la rémunération ? La loi interdit-elle l'acte de neutralisation de la mesure technique d'accès ou les appareils permettant cette neutralisation ? Dans ce dernier cas, quelles activités sont interdites (vent, fabrication, possession, prestation de services, etc…) ?

3. La Directive européenne inclut expressément les services de la société de l'information dans son champs d'application, définis ailleurs comme les services fournis à distance sur demande individuelle du destinataire du service. Votre législation sur l'accès conditionnel couvre-t-elle également les services de la société de l'information ? En d'autres termes, peut-elle être appliquée aux services fournis sur Internet ou sur d'autres services électroniques ?

La loi du 1er août 2000 relative à la liberté de communication prévoit le régime applicable aux exploitants de système d'accès sous condition (article 95 de la loi). Toutefois, ces textes ont surtout pour objet de prévoir les conditions dans lesquelles ces exploitants doivent permettre l'accès à ces technologies sans distorsion de concurrence.

En dehors des textes d'ores et déjà mentionnés (protection par le droit pénal de l'informatique – protection des décodeurs), il n'existe pas de dispositions spécifiques.

4. Droit des télécommunications

Il faut rappeler que le droit des télécommunications repose sur quelques grands principes qui définissent les droits des utilisateurs.
Pour les présenter nous reprendrons la classification effectuée par Monsieur le Professeur Michel Vivant (LAMY : DROIT DE L'INFORMATIQUE ET DES RESEAUX, Edition 2000, n° 1944) :

1. le droit au raccordement du réseau
2. le droit au secret des correspondances
3. le droit à la neutralité de l'opérateur
4. le droit au recours contre les fournisseurs
5. le droit à la protection contre les clauses abusives.

Nous rappellerons également l'existence de la loi précitée du 30 septembre 1986, modifiée par la loi du 16 décembre 1992, qui sanctionne l'accès non autorisé à un programme télédiffusé lorsque cet accès est conditionné par le versement d'une rémunération à l'exploitant du service.

a. Les réglementations relatives aux télécommunications peuvent sanctionner l'interception non autorisée de communication, soit par décryptage, soit par tout autre acte d'accès au contenu lors de sa transmission sur un réseau de télécommunications. Ce type de dispositions pourrait fonder une action contre le décryptage ou l'accès non autorisé à des données transmises sur des réseaux de télécommunications. La loi sur les télécommunications contient-elle une telle interdiction ?

La réponse est affirmative. Une telle interdiction est stipulée par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

1. Quel est l'acte visé ? La loi évoque-t-elle les équipements permettant ou facilitant une telle interception ?

L'article 226-15 du Code pénal sanctionne *« le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications »*.
La loi évoque les équipements puisque le même article 226-15 incrimine également le fait, commis de mauvaise foi, de *« procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »*.

2. Le contenu doit-il être crypté ou autrement protégé pour bénéficier de la protection ?

La réponse est négative. Sont protégées les correspondances de toute nature.

3. L'interdiction d'interception ou de distribution d'équipement la permettant souffre-t-elle de certaines exceptions (par exemple lorsque les appareils de décryptage ou d'interception respectent certaines normes techniques) ?

Non, l'application du texte n'est pas liée à des critères techniques.

4. Qui peut intenter une action sur la base de ces dispositions ? Quelles sont les actions et sanctions prévues ?

Les personnes dont la correspondance a été interceptée, détournée, utilisée ou divulguée, de mauvaise foi. L'article 226-15 du Code pénal prévoit une peine de un an d'emprisonnement et de 300 000 F d'amende.

b. Le droit des télécommunications peut également imposer aux appareils terminaux le respect de certains standards techniques. Ceci pourrait constituer un moyen d'interdire les systèmes des télécommunications permettant la réception non autorisée de communications. Qu'en est-il dans votre législation ?

Un texte impose aux appareils terminaux le respect de certains standards techniques. Il s'agit du décret n° 92-116 du 4 février 1992 relatif à l'agrément des équipements terminaux de télécommunication, à leurs conditions de raccordement et à l'admission des installateurs (LAMY : DROIT DE L'INFORMATIQUE ET DES RESEAUX , Edition 2000, n°1939). Mais ces textes sont déconnectés de la protection des contenus.

5. <u>Criminalité informatique</u>

a. Votre pays dispose-t-il d'une législation relative à la criminalité informatique ?

La réponse est affirmative. La loi n° 88-19 du 5 janvier 1988 dite « loi Godfrain », aujourd'hui reprise dans les articles 323-1 et suivants du nouveau Code pénal (-cf. réponses aux questions précédentes).

Le contournement d'une protection technique ou l'accès non autorisé à un système ou réseau informatique constituent-ils un délit ?

La réponse est affirmative.
L'article 323-1 du nouveau Code pénal dispose que *« le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende »*.

Quel est l'objectif de la criminalisation de tels actes ?

Sanctionner une nouvelle forme de criminalité contre laquelle le recours au droit commun manquait d'efficacité, en raison notamment du principe de spécialité en droit pénal.

b. Comment sont définis les actes qui sont interdits ? La manière dont l'accès non autorisé est rendu possible est-elle spécifiée, par exemple la fourniture d'un faux mot de passe, le décryptage, un autre acte de piratage ?

Les actes interdits sont définis largement. La manière dont l'accès est rendu possible n'est pas spécifiée. En effet, c'est le simple fait d'accéder frauduleusement à un système de traitement automatisé des données qui est incriminé, les moyens employés à cette fin étant indifférents.

c. La loi pénale vise-t-elle également les équipements permettant la commission de tels délits (parfois qualifiés de « hacker tools ») ? A défaut, le vendeur ou le fabriquant de ces équipements pourraient-ils être poursuivis comme complices ? Quelles sont les peines prévues pour ces délits ?

La loi pénale ne vise pas directement les équipements.
Le vendeur ou le fabriquant de ces équipements et/ou toute personne pourraient être poursuivies sur la base des textes généraux relatifs à la complicité.

En effet, l'article 121-7 du Code pénal dispose *qu'«est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation »*.

d. Quels sont les éléments du délit ? Une intention frauduleuse ou un autre élément moral est-il requis ?

Un élément matériel et un élément moral sont nécessaires pour que l'infraction soit réalisée. L'élément matériel consiste en un accès et/ou un maintien non autorisé dans un système. L'élément moral réside dans la connaissance de l'absence de droit à accéder et/ou se maintenir dans le système.

e. Les tribunaux ont-ils déjà appliqué ces dispositions dans le contexte d'une mesure technique de protection ou d'un accès non autorisé à des données ou à d'autres objets techniquement protégés ?

La réponse est affirmative. Toutefois, l'application du texte ne dépend pas de l'existence d'un accès restreint ou soumis à condition. Le simple accès et/ou maintien, dés lors qu'il n'est pas autorisé expressément, est ainsi sanctionné (Cour d'appel de Paris – 5 avril 1994).

f. A défaut d'une loi sur la criminalité informatique, certains délits traditionnels (vol, escroquerie, faux, effraction, etc) pourraient-ils être appliqués à l'accès non autorisé et/ou à la neutralisation d'un dispositif technique ? Existe-t-il des cas de jurisprudence ?

En principe ces incriminations sont susceptibles de s'appliquer à l'accès ou au maintien non autorisé dans un système informatique ou dans un réseau dès lors que l'on entre dans les conditions fixées par les textes.

6. Pratique commerciale et concurrence déloyale

a. Dans votre pays, la commercialisation d'appareils ou d'équipements de décryptage ou de décodeurs a-t-elle été sanctionnée, à défaut d'une protection spécifique, sur la base du droit de la concurrence déloyale ? A quelles conditions ?

Il n'y a pas de cas d'application jurisprudentielle du droit de la concurrence déloyale à la commercialisation d'appareils ou d'équipements de décryptage en droit français.

b. Quels sont les avantages, inconvénients ou limites de l'application du droit de la concurrence déloyale à de telles pratiques ? Cette protection est-elle, selon vous, effective et efficace ?

La finalité du droit de la concurrence déloyale ou des agissements parasitaires est différente. Ce droit est fondé sur une application large de l'article 1382, relative à la responsabilité civile.

Les inconvénients résident dans la difficulté de prouver les éléments permettant d'agir sur cette base, et notamment l'existence d'une faute en l'absence de droits privatifs sur l'objet de la protection.

Cette protection ne peut être efficace, car elle dépend des circonstances de chaque espèce, et n'assure donc pas une prévisibilité suffisante.

Il faut de plus une dilution des protections juridiques spécifiques par l'extension inappropriée de la protection par la concurrence déloyale ou l'agissement parasitaire.

7. Protection du dispositif technique

Le dispositif technique de protection peut lui-même faire l'objet d'un droit privatif. Il peut s'agir d'un droit d'auteur ou d'un brevet sur un logiciel ou encore d'un secret de fabrique ou secret d'affaires qui protège la clef de décryptage ou le mécanisme technique lui-même. Contourner le logiciel ou le moyen technique ou fabriquer ou distribuer des équipements de contournement pourrait constituer un acte de reproduction (décompilation du logiciel par exemple), d'exploitation non autorisée ou une divulgation du secret de fabrique ou secret d'affaires.

a. Votre législation sur le droit d'auteur, les brevets ou le secret d'affaires est-elle susceptible de s'appliquer dans ce contexte ? A quelles conditions ? La jurisprudence a-t-elle déjà protégé un mécanisme technique par ce biais ?

La législation relative aux logiciels peut parfaitement s'appliquer, dés lors que le dispositif technique utilise un logiciel.

Cette protection est assurée aujourd'hui en droit positif par le droit d'auteur, et ne peut être assurée par les brevets, quelque soit les débats actuels sur la brevetabilité des logiciels.

Par ailleurs, le Code de la Propriété Intellectuelle protége d'ores et déjà les dispositifs techniques de protection des logiciels par un texte spécifique (étant rappelé que le droit pénal de l'informatique pourra également s'appliquer).

L'article L 122 – 6 – 2 du CPI dispose :

« **Art. L. 122-6-2** *(Loi n° 94-361 du 10 mai 1994).* Toute publicité ou notice d'utilisation relative au moyen permettant la suppression ou la neutralisation de tout dispositif technique protégeant un logiciel doit mentionner que l'utilisation illicite de ces moyens est passible des sanctions prévues en cas de contrefaçon. Un décret en Conseil d'Etat fixera les conditions d'application du présent article. »

Le décret n'a pas encore été pris, et il n'y a pas de cas de jurisprudence d'application de ce texte.

Par ailleurs, la protection relative aux secrets de fabrique et au savoir faire peuvent trouver à s'appliquer.

Mais ces protections obéissent à des conditions spécifiques, qui viendront sanctionner les agissement ayant permis d'avoir accès à l'information relative au système de protection, et non à l'atteinte relative au système de protection lui-même.

b. Quelles sont les exceptions de ces régimes spécifiques de protection dont pourrait bénéficier la personne qui a contourné ou fabriqué/distribué des dispositifs de contournement ?

Il existe une exception relative à l'interopérabilité du logiciel (article L.122-6-2 du Code de la Propriété Intellectuelle).

Cet article dispose :

« **Art. L. 122-6-1** *(Loi n° 94-361 du 10 mai 1994).* I. - Les actes prévus aux 1° et 2° de l'article L. 122-6 ne sont pas soumis à l'autorisation de l'auteur lorsqu'ils sont nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser, y compris pour corriger des erreurs.

Toutefois, l'auteur est habilité à se réserver par contrat le droit de corriger les erreurs et de déterminer les modalités particulières auxquelles seront soumis les actes prévus aux 1° et 2° de l'article L. 122-6, nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser.

II. - La personne ayant le droit d'utiliser le logiciel peut faire une copie de sauvegarde lorsque celle-ci est nécessaire pour préserver l'utilisation du logiciel.

III. - La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer.

IV. - La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction de la forme au sens du 1° ou du 2° de l'article L. 122-6 est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :

1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;

2° Les informations nécessaires à l'interopérabilité n'ont pas été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;

3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.

Les informations ainsi obtenues ne peuvent être:

1° Ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante ;

2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;

3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur.

V. - Le présent article ne saurait être interprété comme permettant de porter atteinte à l'exploitation normale du logiciel ou de causer un préjudice injustifié aux intérêts légitimes de l'auteur.

Toute stipulation contraire aux dispositions prévues aux II, III et IV du présent article est nulle et non avenue. »

Dans le cadre de cette exception, il serait possible de porter atteinte aux systèmes de protection technique basé sur un logiciel, pour adapter ce dernier à un autre logiciel compatible et/ou à du matériel compatible (Cour d'Appel de Paris, 12 décembre 1997 – interopérabilité pour l'adaptation du logiciel de disquette ZIP à un lecteur) .

Il convient aussi de noter que les tribunaux français ont donné une interprétation très restrictive de la copie de sauvegarde. Celle-ci ne peut être effectué que si l'éditeur de logiciel ne l'a pas fourni, et que si celle-ci est utile.

8. <u>Autres protections</u>

a. Comment pourrait-on protéger les mesures techniques, en dehors des législations ou mécanismes juridiques abordés ci-dessus ? Par quel type de législation ou de mécanismes juridiques (par exemple loi sur la protection des données personnelles et de la vie privée, droit de propriété, etc…) ? Dans quelles hypothèses ?

b. En particulier, pensez-vous que le droit des contrats peut offrir une solution effective pour interdire la neutralisation d'une protection technique ?

1. **Hypothèse d'un contrat géré par la mesure technique elle-même (cas des licences on-line) qui interdirait la neutralisation. Un tel contrat est-il valable ?**

Un tel contrat serait « à priori » valable. Toutefois, un tel contrat ne pourrait pas interdire la décompilation aux fins d'interopérabilité.

Les contrats proposés par les sociétés d'auteurs prévoient d'ailleurs que l'autorisation conférée au titre des droits n'est valable que sous réserve de l'utilisation de certains logiciels, ces logiciels ne devant pas permettre le téléchargement mais uniquement le streaming.

2. **Hypothèse d'un contrat conclu avec l'industrie informatique ou électronique qui les obligerait à développer des appareils qui respectent la mesure technique ou qui ne la neutralisent pas ? De telles négociations ont-elles eu lieu dans votre pays ?**

Nous n'avons pas connaissance de négociations en ce sens, ce qui ne signifie pas qu'elles n'existent pas.

9. <u>Exceptions, droits fondamentaux, intérêts des tiers et intérêt public</u>

a. Existe-t-il des limitations générales aux protections envisagées dans ce rapport, limitations qui s'appliqueraient indépendamment des dispositions juridiques sur lesquelles est basée l'action contre la neutralisation des mesures techniques (limitations résultant par exemple de la liberté d'expression, la liberté d'information, l'intérêt public, la protection du consommateur, l'abus de droit, etc…) ?
b. Quelle est la position, dans votre pays, de l'industrie informatique et électronique ? Leurs produits sont-ils susceptibles d'être interdits sur la base des législations évoquées ci-dessus ? Comment leurs intérêts ont-ils été pris en compte ?

Il faut rappeler ici les droits fondamentaux des utilisateurs précédemment cités :

1. le droit au raccordement du réseau
2. le droit au secret des correspondances
3. le droit à la neutralité de l'opérateur
4. le droit au recours contre les fournisseurs
5. le droit à la protection contre les clauses abusives.

Toutefois, il est clair que de nombreux intérêts divergents devront être pris en compte lors des débats pour la transposition de la directive Droits d'auteur et droits voisins dans la société de l'information.

10. <u>Application des protections envisagées aux questions 1 à 9 aux œuvres protégées par un droit d'auteur</u>

a. **Les titulaires de droit pourraient-ils recourir aux mécanismes et dispositions juridiques évoquées ci-dessus, soit pour interdire la neutralisation des mesures techniques protégeant son œuvre, soit pour interdire la distribution d'équipements permettant ou facilitant un tel contournement ? Quelles protections pourraient s'appliquer ?**

b. **Ces différentes protections sont-elles susceptibles d'être utilisées alternativement ou conjointement à la protection spécifique des mesures techniques dans le droit d'auteur ?**

c. **Quels sont les avantages et les inconvénients pour l'auteur de recourir à ces différentes dispositions légales ? Ces différents régimes juridiques jettent-ils un autre éclairage sur l'opportunité d'une protection nouvelle et spécifique en droit d'auteur ?**

d. Si l'auteur peut recourir à ces protections en dehors du droit d'auteur, cela pourrait-il justifier de réaliser la transposition des dispositions des Traités OMPI en la matière dans des législations autres que le droit d'auteur ? Pensez-vous que cette solution serait opportune et efficace ? Dans la négative, quels sont les manques et défauts de ces dispositions existantes qu'une protection spécifique en droit d'auteur comblerait ?

Avez-vous d'autres observations ?

Les titulaires de droit peuvent aujourd'hui potentiellement recourir à l'ensemble des dispositifs juridiques rappelés dans les réponses au questionnaire.

Toutefois, il semblerait préférable qu'ils disposent de leurs propres règles de protection des mesures techniques.

Tel sera le cas dans le cadre de la transposition de la directive Droit d'Auteur et droits voisins dans la société de l'information.

Trois conditions minimales devraient être remplies pour assurer la protection des mesures techniques.

1 - Une des conditions importantes est que cette protection soit accordée aux titulaires de droits, et non à toute personne intervenant dans la chaîne de diffusion des objets protégés. Il appartiendra ensuite aux titulaires de droits de décider de la manière dont ils souhaiteront mettre en œuvre, notamment par contrat, leurs prérogatives.

2 - Une seconde condition devra être d'assurer l'effectivité de la protection juridique spécifique des mesures techniques en évitant que les bénéficiaires des exceptions puissent revendiquer un droit à ces exceptions, qui neutraliseraient la protection des mesures techniques.

3 - Enfin, il est essentiel que les régimes spécifiques de protection des mesures techniques n'interdisent pas aux titulaires de droits d'utiliser les autres outils juridiques mis à leur disposition dans le droit positif actuel.