6/3/96

LEGAL PROTECTION FOR ENCRYPTED SERVICES IN THE INTERNAL MARKET

CONSULTATION ON THE NEED FOR COMMUNITY ACTION

Commission Green Paper

GREEN PAPER ON THE LEGAL PROTECTION OF ENCRYPTED SERVICES IN THE INTERNAL MARKET

Executive summary

Objective

In recent years the increase in the availability of frequencies and the use of new technology have been accompanied by an increase in the number of television services whose signal is encrypted with a view to restricting reception to subscribers. In order to receive the programmes, viewers must have a decoding device that can reconstitute the original picture.

The market is experiencing rapid growth particularly as a result of the advent of digital technology, which permits an expansion in the capacity for communication. These television services will increasingly be compelled to adopt a transnational and often even European dimension due to their specialised nature. However, growth is being jeopardized by piracy: a flourishing unofficial decoder manufacturing industry is emerging in parallel to that of authorised manufacturers. Devices enabling access to a service without payment of the subscription or fee are produced and marketed without the permission of service operators. This results in considerable losses for the service provider and indirectly adversely affects the potential market of programme suppliers and official manufacturers.

In the light of these developments, the Commission already emphasised the need for effective protection of coded signals against their illegal reception in its Strategic Programme for the Internal Market of 22 December 1993 (COM(93)632 final).

Such a requirement is all the more urgent in the run-up to the Information Society: as more and more encrypted services become available in the future, measures will need to be adopted to ensure the protection of these services, whatever their content, against illicit reception.

Accordingly, in its Communication of July 1994 entitlted "Europe's Way to the Information Society: An Action Plan" (COM(94) 347) the Commission announced the preparation of a Green Paper on the Legal Protection of Encrypted Services in the Internal Market with the aim of examining problems raised both by the absence of specific legislation on the legal protection of encrypted services in some Member States and by disparaties between existing legislation in others.

The current regulatory environment

A comparison of the regulatory methods chosen by legislators in the Member States reveals appreciable differences in the approach to the problem of illicit reception of encrypted services.

Whereas some Member States adopted *specific legislation* ensuring protection against the illegal reception of encrypted services in the late 1980s, others (A, P, E, GR, DK, D and LUX) have no such legislation to date.

The general rules (e.g. on unfair competition, telecommunications and copyright) sometimes applied in Member States belonging to the second group are often unable to provide effective protection against the illegal reception of encrypted services. This has allowed the development, in some of those Member States, of a flourishing industry that manufactures, markets, installs and maintains pirate devices. A specialist

press has also developed, providing targeted publications and commercial promotion networks for pirate decoders. The repercussions of this situation extend to other Member States, where such devices are introduced on to the market in spite of restrictive measures.

Among the Member States which have adopted specific legislation, *the differences between the solutions adopted* are substantial, in particular as regards scope, the activities prohibited (commercial promotion, private possession) and the level of sanctions.

Need for Community action

In view of this situation, *Community action could well be justified*. The fact that the Member States do not all have an equivalent level of legal protection *prevents the Internal Market from operating correctly*. This creates a number of obstacles to the free movement of encrypted services and decoders and numerous distortions of competition between operators in the various Member States. The present differences between the regulatory solutions *a*nd the resulting extra costs and legal uncertainty are viewed by the profession as a *major barrier to the development of a European market of new encrypted services*.

Such an initiative would also be useful in preparation for the *Information Society*, in which encrypted services could be called upon to play a major role. It would also eliminate the fragmentation of the Internal Market and would simultaneously take other existing Community objectives into account such as those persued by the *industrial, audiovisual, cultural and consumer protection policies*

Operators have overwhelmingly expressed support for a Community measure. In this regard, the *DVB (European Digital Video Broadcasting Group)* has adopted a recommendation emphasizing the need for a clear and uniform EU-wide regulatory framework. This view was shared by the *European Parliament*, which proposed inserting in the Directive on the Use of Standards for the Transmission of Television Signals a recital underlining the need to introduce and apply efficient anti-piracy legislation at European level; the Directive, along with the recital, was adopted by the *Council* on 24 October 1995.

Before proposing an initiative, however, the Commission would like to consult interested parties on the course of action described below.

The Commission could propose an *initiative harmonizing national legislation*. Taking into account the principle of proportionality and subsidiarity, the proposed initiative could provide for minimum harmonisation, leaving Member States free to adopt stricter principles while ensuring a *minimum level of equivalent protection* within the Union. The proposed initiative could thus prohibit the production, sale, possession for either commercial or personal use, installation and commercial promotion of decoders designed to enable access to encrypted services without the encryptor's authorisation. Such a course of action would both ensure EU-wide equivalent protection against illicit access to encrypted services and afford legal certainty to the interests concerned.

Next step

The Commission is keen to ensure that the Green Paper is the subject of *open consultations*: any person, firm, body or authority is free to take part. This will be a twin-track consultation process, in that it is addressed not just to trade associations and federations but also to individual operators. The Green Paper will be sent to the European Parliament, to the Economic and Social Committee, to the Committee of the Regions, to the Member States, to the European Economic Area and to the countries of Central and Eastern Europe.

The time-limit for submitting comments is 31 May 1996. In the summer of 1996 the Commission will, in the light of the comments received, decide whether an initiative at Community level is called for.

Introduction

I. The problem of illicit reception

The use of *signal encryption* in broadcasting has been on the increase in recent years. In the 1980s systems characterised by varying degrees of security began to appear employing a form of scrambling in which the standard picture and/or sound signals are altered before transmission in such a way that a normal receiver cannot reconstitute the original programme. In order to recover the original picture the viewer needed a *special decoding device* (decoder, smart card or computer programme-normally issued on the payment of a subscription fee) which could interpret the instructions accompanying the encrypted signal.

Originally used by cable companies to modulate the number of channels available to the viewer under the terms of his subscription agreement, the technology rapidly spread to terrestrial pay-television stations and evolved dramatically with the satellite broadcasting of encrypted channels. The use of encryption will, however, increase sharply with the advent of digital technology and the development of Information Society services (such as interactive teleshopping, tele-information services, on-line professional services and interactive games) since they will all, in varying degrees, need to rely on encryption to ensure their viable development.

Encryption is used for a variety of reasons: *on top of commercial strategy requirements*, i.e. the need to find *fresh sources of revenue*, copyright holders can require to use encryption to *protect and exploit the covered programmes*. *The protection of minors*, particularly in the case of adult channels, as well as the improved identification of the audience to allow for targeted maketing, can also be major factors.

A flourishing *unauthorised manufacturing* industry has, however, sprung up alongside that of official producers of decoding devices. This pirate industry manufactures and markets decoding devices enabling *illicit reception of the service without the service provider's authorisation* , usually at prices below those of official devices.

It is estimated that unauthorised devices currently represent about *5 to 20%* of the total number of devices in circulation and generate turnover of several million Ecus annually. Moreover, a specialised press developed around this pirate market, providing targeted publications and thus also a medium for the marketing of unauthorised devices. An after-sales service market also developed, providing maintenance and even sometimes the replacement of the device in the event that the operator would change system.

The sale of these unauthorised devices has, first of all, an adverse effect on the *operators of encrypted services.* As well as suffering losses in terms of potential market and profits, they bear additional costs as a result of having to adopt expensive distribution systems for their decoder devices (which are usually rented out) in order to control their use.

For *the suppliers of the programmes contained in the broadcasts*, the marketing of the unauthorised devices represents a loss of profits, as in the negotiations concerning the price payable for the rights,

no account will have been taken of the individuals who receive the programmes via an unauthorised device.

For those *supplying the technology*, the marketing of unauthorised devices undermines confidence in their system and results in lost profits connected with the potential market taken over by such equipment.

For the consumers, the marketing of the unauthorised devices constitutes a risk as they could be mislead about the origin of the decoding device they are purchasing and thus believe they are buying authorised device, whereas it is in fact a pirated decoder. In this case, if the operator modifies the encryption system for security reasons, the device purchased would be of no use to the consumer, who would have to pay for another decoder. Moreover, the service providers pass on the losses they suffer from piracy onto the price of, or rental charges for, authorised devices made available to consumers.

II. The Regulatory Environment

In order to redress this problem, operators have asked that Member States adopt specific rules providing *rapid and effective legal protection* against the manufacture and distribution of unauthorised decoding devices. While *technological progress* has improved the security of encryption systems, purely technological solutions have often proved ineffective. When choosing an encryption system the operator is faced with a trade-off between the cost of the system and the level of security it provides. Experience has moreover shown that piracy techniques have developed at the same rate as encryption techniques and that there is no guarantee that new systems using digital technology will not come under attack. It was therefore felt that, in order to deal with pirates, technology had to be supplemented by legislation. However, the resulting *wave of regulatory change among Member States*, which has not as yet been completed, reveals a substantial difference in approach.[1]

In this context, in its July 1994 Communication entitled "Europe's way to the Information Society. An Action Plan" (COM(94) 347), the Commission announced the preparation of a *"Green Paper on the Legal Protection of Encrypted Services in the Internal Market"* aimed at analysing the problems raised both by the absence of specific legislation on illicit reception of encrypted services in some Member States and by disparities between existing legislation in others.

III. Services covered

The subject of the following analysis is *the illicit reception of an encrypted service*, i.e. reception without payment and/or authorisation,by persons who are not authorised by the service providers, and the solutions that have been found to this problem by national regulations. *"Encrypted services"* is defined for the purposes of this Paper as services whose *signal is encrypted in order to ensure payment of a fee*. This category includes *traditional encrypted broadcasts* (via a cable, hertzian waves or by satellite), the *new broadcasting services* (digital television, pay-per-view, near video on

[1] See Chapter 3: Member States' legislation.

demand) and *Information Society services*, namely electronic distance services provided on individual request of a service user (in particular video on demand, games supplied on request, teleshopping and multimedia information services).

Services encrypted for reasons other than ensuring the payment of a fee, i.e. those encrypted in order to guarantee the *integrity and confidentiality of the message transmitted*, namely financial or telecommunications services (in particular mobile telephone services using GSM technology) are not covered. This exclusion is based on the fact that *the general interests* involved in the event of interception of these services (i.e. the integrity and confidentiality of the communication) differ appreciably from the general-interest objective (i.e. the protection of the value of a service provides against payment) threatened by the illicit reception of encrypted services as defined for the purpuse of this Paper. As this difference has led to *appreciably different solutions in terms of legislation* both at national and international level particularly as regards action and the level of sanctions, the joint treatment of both problems is not justified.

Moreover, the Green Paper does not cover questions concerning systems designed to prevent the *copying* of a work or other protected subject matter. These have been addressed in the Green Paper on Copyright and Related Rights in the Information Society adopted by the Commission in July 1995.

Lastly, this Green Paper does not deal with questions relating to the *standardization of conditional access systems*, or with the conditions under which licences are granted for such systems, since they are already covered by the Directive on the Use of Standards for the Transmission of Television Signals,[2] or *with the control by national authorities* of coding systems. The latter question, which is closely linked to the the problem of *security*, is currently being studied by the Commission in the context of its work on the security of information systems. Other studies could furthermore be launched at a future date if the efficient operation of the Internal Market would be threatened or jeopardized by the implementation of national rules.

IV. Preparatory work

In preparation for the Green Paper, the Commission asked three independent firms to examine the technological, economic and legal aspects of the market in encrypted services.[3]

---

[2] Directive 95/47/EC of the European Parliament and of the Council of 24 October 1995 on the Use of Standards for the Transmission of Television Signals (OJ No L 281, 23.11.1995, p. 51).

[3] Copies of their findings are obtainable from:
European Commission,
Directorate-General for the Internal Market and Financial Services,
The Media, Commercial Communication and Unfair Competition,
DG XV/E/5
C 107 8/59
200 rue de la Loi
B 1049 Brussels
Belgium
Fax: (32-2) 295 77 12
Email: e5@dg15.cec.be

The first study, *"Technical aspects related to encrypted broadcasts"* concentrated on the economic and technical aspects of the subject and dealt in particular with currently used encryption systems, their advantages and disadvantages and their vulnerability to pirate activities. As regards the economic aspect, the study focused on the cost of the managment of a subscribtion system for encrypted services, on the trend towards the development of compatible decoding systems and on the advent of the new digital technologies.

The second study, *"Protection of encrypted broadcasts"* concerned the legal aspects of the issue. It analysed the factors which influenced the development of encrypted services, the reasons for piracy and the legal solutions adopted to combat it.

The third study, *"Legal protection of encrypted broadcasting signals"* examined the legislation of the Member States on the protection of encrypted broadcasts, application of these laws by national courts and, where relevant, the established controls and sanctions. The Institute also analysed the regulations adopted by international bodies (Council of Europe, WIPO).

In addition, in March 1995, the Commission initiated a wide-ranging process of consultation with the relevant sectors of industry concerned with the problem of illicit reception of encrypted services, particularly broadcasters, manufacturers of decoding devices, cable operators, programme providers, telecommunication companies and other interested parties who had expressed a desire to be involved.

The consultation confirmed that *illicit reception of encrypted services* and *fragmentation of the legal framework at the level of the EU* pose a real problem for the media industry. It believes that the possibility of benefiting from effective legal protection against illicit reception is an important factor when deciding on the distribution of a new encrypted service in a particular Member State. *In the absence of such protection, operators often prefer not to market the service*.

Operators thus overwhelmingly expressed support for a Community initiative. Similarly, in 1995, in the context of the meeting of its group of experts, *the DVB (European Digital Video Broadcasting Group)*, which is at the forefront of digital television standards, adopted a recommendation underlining the need for a clear and uniform EU-wide regulatory framework which can be relied upon in the event of illicit reception of encrypted services.

That view was shared by the European Parliament, which, in the procedure leading to the adoption of the Directive on the Use of Standards for the Transmission of Television Signals[4] proposed inserting a recital emphasizing that, in a digital environment, the scope for piracy in the European audiovisual market will increase, with negative consequences for both operators and programme providers, and that it is becoming increasingly necessary to introduce and apply efficient anti-piracy legislation at European level. The recital was adopted along with the Directive by the *Council* on 24 October 1995.

---

4 Directive 95/47/EC (see above).

Chapter 1: The European market in encrypted services

1. A buoyant market

The recent past, *technological developments* (e.g. satellites and fibre optic cables) have produced rapid changes in the European audiovisual landscape and allowed for a steady expansion of the supply of services. As more operators have increasingly engaged in *targeted commercial strategies*, the encryption of their signals has proved essential for their viability.

The traditional structure for financing private channels, based exclusively on advertising income, is often no longer a viable proposition for new entrants. As the number of broadcasting stations increases, the contribution of income per channel from traditional television advertisers becomes smaller. Simultaneousley operators attempt to distinguish themselves from this growing number of potential competitors by catering to the needs of specific *market niches*, i.e. by focusing on the tastes and interests of particular user groups (thematic film, music or sports channels, etc.). An operator can thus profile himself from his mass market competitors by targeting a demand that had previously been satisfied only in part or not at all. Comparing identical geographical areas, however, niche service audiences are invariably more closely targeted and, by the same token, smaller. Operators of specialised media cannot, therefore, rely on income from mass market advertisers,[5] who express less or little interest a media strategy that is not aimed a mass audience.

1.1 Reasons for using encryption:

The main reasons for encrypting signals can be summed up as follows:

- *To ensure the financial contribution of the beneficiaries of the service:* the concept of niche services is based on the ability to provide added value to certain categories of users as compared to those aimed at the mass market. Users can therefore be asked to contribute to the financing of this specialised service which, as a result of encryption, cannot be received by non-subscribers;

- *The possibility of increasing advertising revenue per audience unit:* by encrypting the signal, the operator will find it easier to sell advertising space to, or strike sponsorship deals with, firms interested in the targeted market niche. Advertisers will therefore be asked to pay for the targeted market only and not for the entire equivalent geographical market. They will therefore be willing to pay more per audience unit since the audience will be regarded as being of a higher quality compared to a mass audience.

- *The ability to target supply more accurately:* increased knowledge of the user of the service will help the operator to fine-tune his service to the exact requirements of the target market.

---

[5] In this document, "advertisers" means firms that make use of commercial communication. This includes all forms of publicity, commercial promotion, direct marketing, sponsorship and public relations. This general approach is preferred since it can take into account recent and possible future changes in the use of marketing tools in the wake of developments in the media field.

- *Simplifying the acquisition of broadcasting rights:* satellite broadcasting has considerably increased the potential reception area. Traditionally, however, broadcasting rights are granted on a territorial basis, which means access often has to be limited to viewers within a specific geographical or common language area. Encryption allows the operator to restrict the reception of the signal exclusively to those territories for which rights have been acquired. Moreover, as suggested in the "Cable and Satellite" Directive,[6] encryption will enable the use of the actual audience (e.g. the number of subscribers and not the geographical area) as a basis for the negotiation of satellite broadcasting and cable retransmission rights, thereby reducing the acquisition cost of programmes intended for the development of a niche service.

- *The creation of a new window in the chronology of media distribution:* encryption allows rightholders to add a new window to the pattern of media distribution; operators of an encrypted service often carry programming before it is broadcast to a mass audience and, in order to secure exclusive rights in respect of those works, they are prepared to pay large sums, thereby creating a new source of income for the rightsholders.

- *Regulatory requirements:* on grounds of public policy, in particular *the protection of minors* (e.g. in the case of broadcasting channels aimed at adult audiences), the authorities may, as forseen in the Television Without Frontiers Directive[7] (Article 22, second sentence), allow certain services to operate on condition that they are encrypted so that reception can be limited to specific groups of viewers.

1.2 Encrypted services

The European market in encrypted services consists mainly of *pay-television channels*[8]. Initially tranmsitted via cable and hertzian waves, this service especially expanded when medium powered and high powered satellites were introduced allowing broadcasts to be received anywhere within the footprint of the satellite using an individual satellite dish.

The development of technology has, however, enabled more sophisticated pay broadcasting services to be launched, e.g. *pay-per-view broadcasts*,[9] which must be

---

6 Council Directive 93/83/EEC of 27 September 1993 on the Coordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission (OJ No L 248, 6.10.1993, p. 15).

7 Council Directive 89/552/EEC of 3 October 1989 on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities (OJ No L 298, 17.10.1989, p.15).

8 "Pay television" is a term used to define a situation in which a viewer pays to receive a particular station hertzian, by satellite and/or by cable.

9 In the United States, 35% of the homes that subscribe to cable (i.e. about 20 million) are equipped with devices enabling them to receive these services. In France, Multivision offers two pay-per-view services to 220 000 homes.

paid for before they can be seen by viewers. Pay-per-view is technically possible without digital compression, but it requires a sophisticated subscription management system. Pay-per-view could involve the viewer paying to see one particular event (e.g. a concert or a boxing match) or a series of events (e.g. the right to see ten football matches). In the latter example the broadcaster cannot presently identify exactly which events have been viewed by a particular viewer. Technological progress is however allowing systems to be developed that will allow rights holders to be remunerated in line with the actual "consumption" of their programmes.

The next stage will probably be *near video on demand*, which involves the broadcaster transmitting the same programme (usually, but not necessarily, a film) at different starting times. A viewer can thus choose not only the programme he wants to see but also, within certain limits, the time at which he wants to see it. This stage will be followed by the commercial development of actual *video on demand*, which gives the viewer complete flexibility over starting times, as they would no longer be pre-determined by the broadcaster.

The explosion of encryption applications will only take place, however, with the development of the other services of the Information Society: not only audiovisual services, but all the other applications (e.g. *interactive teleshopping, tele-information services, professional on-line services, interactive games, etc.) will, to a varying degree, have to rely on encryption for their viable development.* Moreover, as encryption will often be essential for security purposes (e.g. for electronic payment in the case of teleshopping), synergy between these two encryption applications (control/security being enhanced by the subscription system) would - under conditions of legal certainty - make its use even better suited to promoting the development of all services in the Information Society .

The development of these new services will depend to a large extent on the establishment of a regulatory framework which simultaneously takes account of the legitimate requirements of operators and users of the services. In this respect, great importance will be attached to the solution found on the international and worldwide level to the multitude of security problems implied in the use of electronic transactions. These include in particular the regulatory restrictions on the use of encryption systems, public authorities' control over encrypted communications for reasons of national security, and the identification and verification of the respective parties. At present, the Commission, in the framework of its activities on the security of information systems, is analysing the possibility of establishing, at European level, organisations which would be responsible for the control and certification, and totally independent from public authorities.

2. The European market

Europe currently has a total of 180 television channels, transmitted via 27 satellites.[10] Many of those channels (79) use some form of encryption (see Table 1) and are

[10] European Audiovisual Observatory: 1994/95 Statistical Yearbook on cinema, television, video and new media in Europe, Strasbourg (1994).

thematic rather than general (e.g. children's programming, sports channels, movie channels, etc.).

Table 1: Number of subscribers to the main pay-television stations ('000 viewers)[11]

	A	B	CH	D	DK	E	Eir	F	Fin	I	L	NL	P	S	UK
Canal Plus								3700							
Sky Movies Movie Channel															2587
Sky Sports															2579
Canal Plus Esp.						893									
Première	35			850											
Filmnet		150			100							160		230	
Telepiù										650					
Sky Multichannel															481
TV 1000					45									230	
Adult Channel				5				5		5					167
Canal Plus TVCF		152													
Canal Satellite France								142							
Filmmax														80	
Tele-TV									8					41	
Teleclub			90												
Canal Satellite Esp.						10									
Lumière TV														31	
Multichoice												2			
Total	35	302	90	855	145	903	0	142	8	655	0	162	0	612	5814

In the future, a sharp increase in the supply of encrypted services can be expected at the European level. The launching of new, completely digital satellites (e.g. Astra 1e and 1f) and the spread of fibre optic networks will enable existing operators presently on the market to increase their supply. Several operators have already announced details of their plans to launch packages of digital channels. The Nethold Group, for instance, which controls Filmnet, will soon launch 150 digital channels, 50 of them offering films on demand. BSkyB plans to launch between 16 and 32 pay-per-view stations towards the end of 1996 as an initial step towards the launch of genuine video-on-demand services. Canal Plus will also soon provide a package of over 20 digital channels. In addition to the services already available they will provide a pay-per-view service, video games and digital radio services. Furthermore a number of French channels, including TF1, Arte and La Cinquième, will cooperate in the launch of a package of digital channels using the same satellite. Lastly, TF1 will launch a package of services ranging from video on demand to interactive programmes via five Eutelsat-based transponders.

[11] Source: European Audiovisual Observatory: 1994/95 Statistical Yearbook on cinema, television and new media in Europe, Strasbourg (1994); Libération "Les comptes décryptés de Canal+", L'Evénement (4 November 1994).

New operators, in particular telecommunications companies, can also be expected to enter the market of Information Society services: British Telecom has already set up a pilot project in which 2 500 homes can, on demand, receive teleshopping, video-on-demand, video games and other services.

At present, many channels still cover a particular common language or geographical market. Nevertheless it is clear that, in the future, national markets will increasingly prove too limited. There will therefore be a growing need for easy cross-border access, for this and the following reasons:

- *As the number of encrypted services rises*, operators will increasingly have to provide more finely targeted services to satisfy the needs of the market. Since these particular demands will not satisfactorily be catered for yet, a niche market could be drawn around a population segment prepared to pay for the added value offered by the service. With the increase in general-interest programming broadcast "in clear", encrypted services have developed to satisfy an increasingly specialized demand, therefore justifying the need for their remuneration by the final user. Nevertheless, the development of viable, targeted services requires a market of a certain size, and as for identical geographical areas, a niche-service market is smaller than a mass-service market, *it can often only be constituted by exploiting a larger geographical market.*

- *The ability to better satisfy linguistic and cultural requirements*. By means of the new technology, the same channel can be broadcast simultaneously in several languages by providing separate soundtracks. In addition, the strategy of interactive services will increasingly be based on specialized services and/or the supply of packages of services. The first will often satisfy the demand of transnational niches, i.e. demand based on factors other than purely national culture, while the second will allow the user to choose what he wants to see. Thus, with the incorporation of advanced information technology, the service provider will be able to offer the widest possible choice including in his package of services films or programmes that take account of national differences.

- *The evolution of technological applications*. Constant improvements and the continuous incorporation of audiovisual service distribution systems by the commercial application of new technologies (satellite broadcasting, optical fibres, the development of the ISDN network (Integrated Services Digital Network) at European level so as to link up with IBC (Integrated Broadband Communication networks) make these services increasingly independent of the distance between the service provider and the user.

- All the regulatory work aimed at the *gradual liberalization* of telecommunications (in particular for satellite and cable) and the *harmonisation* of cross-border rules on the carrying of signals in Europe (especially for television signals in the field of programme content and copyright) is just beginning to have a positive impact on the freedom to provide existing

audiovisual services between Member States and the development of new services, a growing proportion of which will be provided in encrypted form.

- *Changes in the practice of granting broadcasting rights*: at present only a small proportion of the output of encrypted stations can be broadcast across frontiers, because of the traditionally national systems of granting broadcasting rights. Encryption will enable future rights to be granted on the basis of the actual number of users rather than according to national frontiers.

- *Obtaining the best possible return on transponder costs*: since transponder costs are high, it is economically sensible for the operator to offer his service in as many areas as possible within the area covered by the satellite.

The development of these services in response to the growing needs of cross-border markets is, however, being jeopardized by a major problem at European level: piracy.

3. A market exposed to piracy

3.1 Technological development

Due to advanced technology, it is in theory now possible to use a conditional access system providing such a high level of security that pirates would be incapable of breaking it. In practice, however, these systems also have to comply with certain economic and regulatory realities, namely:

- Systems must be produced and distributed at a *reasonable price*, since consumers will be unwilling to pay more than a certain amount to buy a decoder,[12] depending on the extent to which they find the programmes interesting or the selection of channels that can be picked up with the system in question.

- The *cost of operating* the system must not exceed the amount of revenue (i.e. the income the operator stands to lose if illicit decoding devices are put on sale) at risk.

- Systems must comply with *regulatory requirements* imposed by certain Member States on the use of encryption for commercial purposes.

As the need to achieve an acceptable cost for the conditional access system means that they cannot be made completely secure, manufacturers of illicit decoding devices have taken advantage of this situation, and are now even able to keep up with the pace of technological developments.

The way in which the systems have evolved illustrate this phenomenon. *The simplest conditional access system* causes a mix-up of the position of the synchronous pulses

[12] Some encryptors have preferred to rent, rather than sell, decoding equipment to their subscribers. This allows them to distribute the devices at a price which is within the reach of more people and to ensure the return of the equipment when the subscription expires.

that form part of the broadcast signals, so that a standard receiver can no longer lock its line (horizontal) or field (vertical) timebases. The picture waveform is transmitted unchanged, but without normal synchronous pulses, the screen displays only a jumble of picture components. The synchronizing information is transmitted in a disguised form (algorithm) which can be detected by the official decoder and used to reconstruct standard synchronous pulses. This system has already been widely pirated.[13]

Second-generation encryption systems work differently. Two of these are now particularly common:

- in the *"active line rotation"* method the line stays in place, but is cut at randomly chosen points for each line and the ends are swapped over;

- in the *"line shuffle"* method the lines that make up the picture are reconstituted in a totally different order. This method is more effective than the first, but also more expensive, as it needs more storage in the decoder.

The great advantage of both systems is that they completely destroy the structure of the picture. They can, moreover, be used in conjunction with a *"smart card"* that "reads" the incoming signal and issues instructions to the decoder telling it how to decode it. The three most widely used encryption systems in Europe (Videocrypt, Syster and Eurocrypt) belong to this second generation.

Research is still being carried out, however, into systems that provide even more security. The current process of the convergence of telecommunications and audiovisual services and the application of digital technology to broadcasting will allow encryption systems to be developed that are more and more sophisticated and secure. After all, the decomposition of content into bytes is in itself a form of encryption.[14]

Moreover, in order to allow the introduction of interactive services, decoders themselves will gradually become "set-top boxes", i.e. actual computers controlled by a smart card that will both identify the user and activate encryption functions for the incoming and outgoing signals. These devices will thus make it possible to pick up the signal, decode it, perhaps change its contents and incorporate it into another medium, record it and print it. They will also be able to interact with traditional equipment (video tape recorders, computers, CD and the new video disc players), and to send back to the operator an encrypted signal, perhaps with confidential financial data, designed to help analyse demand.

3.2 The consequences of piracy

[13] The pirate decoders are believed to reconstruct the sequence of delays by monitoring the start point of successive active lines. A decoder design was even published some years ago in the French press.

[14] The standardization of encryption systems for digital broadcasting that has taken place in the context of the work of *DVB (Digital Video Broadcasting Group)* is a major step towards the general use of encryption technology and an increase in the level of security.

In some Member States, however, the manufacture and marketing of unauthorised decoding devices and the manipulation of authorised devices so as to allow access to a service in breach of the conditions laid down with regard to time (duration of the subscription) and quantity (number of channels) have now become highly lucrative.[15] In those Member States, they have given rise to parallel activities, such as the publication of specialized magazines and the setting-up of maintenance and after-sales services.

The fact that they allow *illicit reception of encrypted services* has several adverse consequences:

- the encryptors are deprived of the subscription revenue they would have obtained if the customer had purchased a lawful device (about ECU 200-250 annually for each unauthorised receiver);

- in some cases it is necessary to replace the pirated system. Operators spend vast sums each year (from ECU 60 000 to more than ECU 1.2 million per operator, according to the survey) on system protection (controlling distribution, making improvements, changing cards, etc.). Even control systems based on removable smart cards, which seemed more immune than most, have been compromised. It was at first claimed that if a system was pirated, it could be safeguarded simply by a new issue of cards. In fact, when the number of subscribers is very large, the cost of replacing all the cards can be a significant drain on earnings. On top of the cost of each smart card,[16] there are the code development costs, postage and other costs (the survey revealed that making pirated systems secure again can cost more than ECU 45 million);

- *the time needed to develop a new system*. Turning once again to the example of the smart cards, an operator wishing to replace its card would need some time to develop a new one. Meanwhile, the only available course of action would be to engage in a series of temporary electronic countermeasures until it can issue a new smart card. This is a risky situation, especially since pirates anticipate the countermeasures and take appropriate avoiding action. In addition, there would inevitably need to be a period of time in which both the old card and the new card would remain operational. This means that the pirate cards in circulation would also last through the transition period, giving pirates enough time to develop a new pirate card. With the assistance of private investors, pirates can now produce their own cards and chips almost as quickly as the broadcasters. Other techniques aimed at disabling pirate cards (e.g. sending de-activating signals that disconnect only unauthorised cards) have proved short-lived (in this particular case, because pirate manufacturers themselves distribute devices specifically designed to block out the de-activating signal).

- financial harm to *those holding rights in the programmes*. Since the *fees paid to rightholders* generally also take into account the *potential audience*, the fact that encrypted programmes are picked up via illicit reception deprives

---

15 It is estimated that unauthorized decoding equipment now accounts for 5-20% of the total market.

16 Between ECU 5 and ECU 25.

rightholders of the income they would have received from subscription revenue if the customer had purchased an authorised decoder instead. Moreover, when negotiations take place regarding rights in respect of subsequent (in clear) broadcasts, rightholders will find it more difficult to secure high levels of remuneration because of illicit reception which had already occurred when the material was broadcast on the encrypted channel;

- the loss of income and credibility for *suppliers of the technology*. When selecting an encryption system, operators will want to be sure that the system chosen is the most secure, so that they can provide those holding the rights in the programmes with a guarantee that a broadcast they have authorised will not be pirated; a high incidence of illicit decoding devices might be construed as evidence that a system is not very effective;

- the fact that *market confidence in the system would be undermined*. The market requires confidence in encryption if the notion of exclusiveness associated with the services is to be maintained and if the window created in the media chronology is to be justified. Illicit reception erodes that confidence in such a manner that rightholders will become reluctant to license first-run programming, broadcasters will not be prepared to pay high licence fees and consumers will be reluctant to pay subscription fees.

- the consumers could be mislead about the origin of the decoding device they are purchasing and thus believe they are buying authorised device, whereas it is in fact a pirated decoder. In this case, if the operator modifies the encryption system for security reasons, the device purchased would be of no use to the consumer, who would have to pay for another decoder. Moreover, the service providers pass on the losses they suffer from piracy onto the price of, or rental charges for, authorised devices made available to consumers.

As well as these direct consequences there are indirect effects on the development of the market in new encrypted services. Clearly, development will be possible only if an adequate level of security is guaranteed for operators to be willing to engage in activities requiring heavy initial investment.

4. A market covered by fragmented rules

In order to deal with the pirate industry, technology has had to be supplemented by legislation as part of a regulatory process at Member State level. This process has followed different approaches and is still not complete. The legislation will be examined in Chapter 3.

According to the media industry, such *regulatory fragmentation* could well entail difficulties for the development of encrypted services at European level and adversely affect the proper operation of the Internal Market. Since the transnational dimension will become increasingly necessary for the growth of a truly European encrypted services industry, the absence of an equivalent level of legal protection against piracy could well have an adverse effect on the development of those services on a European scale.

As confirmed by the consultation, operators could, because of the absence of legal protection in one or more countries where reception is possible, decide not to cover a Member State, for fear of the consequences of piracy in that country. Effective legal protection weighs heavily in an operator's decision to market his service in a given Member State.

In addition, the cost of research into national laws and of possible legal proceedings in the event of piracy in the various Member States means additional costs to operators and to their activities, thus adversely affecting the development of the service.

When negotiations covering programme rights take place, the absence of equivalent legal protection in every Member State where reception is possible will make it more difficult to secure those rights since (especially in the case of recent works) operators cannot guarantee that there will be no illicit access in other Member States. It will also be more difficult to determine what remuneration the rightholders should receive, given that the actual audience in the signal reception area cannot be determined accurately. Operators will thus find it more difficult to secure rights at a reasonable price, and this will have repercussions on their cross-border activities in particular.

Since certain methods of transmission are more exposed to illicit access than others (in particular off-air or satellite transmission as compared with cable distribution, which is generally more secure due to the physical link with the viewer), operators may well choose not to use some of those methods feeling that the risk of piracy is higher. Thus, in the absence of effective legal protection, certain transmission systems, in particular those with the strongest transnational potential, might be used less often than others.

The absence of equivalent legal protection in Member States will also have negative consequences if illicit equipment is imported from third countries. Such equipment will be able to enter the Community via a Member State which does not prohibit its marketing or distribution and can then easily arrive in another Member State, making the latter's efforts to combat illicit reception ineffective.

What is more, the disparity between rules on illicit reception will result in distortions of competition between operators in different countries. Those who transmit signals in Member States providing a high level of legal protection will have a competitive advantages (this will be reflected in their programme-purchasing ability, for instance) over those who distribute their signal in a State where there is no legal protection, since they will have to bear additional costs through having to use a particularly secure encryption system.

Lastly there is a risk that, as a result of differences between solutions in the Member States, the opportunities afforded by the Directive on the Use of Standards for the Transmission of Television Signals[17] will be lost. The use of increasingly standardized systems will be hindered by the fact that the level of legal protection against illicit access is not the same in all the Member States from which the programmes are broadcast. This means that the level of security of the system and the means used to distribute decoding equipment will have to vary with the Member State

[17] Directive 95/47/EC (see above).

of reception, leading to further fragmentation in an audiovisual area which, to some extent, ought to be standardized. In this respect, *DVB (European Digital Video Broadcasting Group*, which is at the origin of the digital television standards partly reproduced in Directive 95/47/EC has, in the context of its experts' group on the piracy of encrypted services adopted a recommendation underlining the need to provide operators throughout the Union with a clear and uniform regulatory framework that can be relied upon in the event of illicit access to encrypted services.

Chapter 2: International rules

1. Recommendations of The Council of Europe

In September 1991 the Council of Europe adopted and addressed to its Member States a Recommendation on the *legal protection of encrypted television services*.[18] The Recommendation was later updated by another, adopted in January 1995, on measures against sound and audiovisual piracy.[19]

In the preamble, the Council of Europe emphasizes the benefits of the development in Europe of pay television on the European audio-visual production sector. The Council of Europe recognizes that encrypted broadcasting services contribute to the diversity of programmes offered to the public, increase the possibilities of exploitation of protected works and are likely to increase the sources of financing of works and programmes in Europe.

The Recommendation goes on to highlight the adverse consequences of illicit access to encrypted broadcasting services and sets out the range of activities which are to be considered unlawful:

- the manufacture of decoding equipment where manufacture is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organization;

- the importation of decoding equipment where importation is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organization;

- the distribution of decoding equipment where distribution is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organization;

- the commercial promotion and advertising of the manufacture, importation or distribution of decoding equipment referred to above;

- the possession of decoding equipment where possession is designed, for commercial purposes, to enable access to an encrypted service by those outside the audience determined by the encrypting organization.

Member States are free to determine that possession of equipment for private use is also to be considered as an unlawful activity.

The Recommendation defines an *encrypted service* as "any television service, transmitted or retransmitted by any technical means, the technical characteristics of

---

[18] Recommendation No R (91) 14 of the Committee of Ministers to Member States on the legal protection of encrypted television services.

[19] Recommendation No R (95) 1 of the Committee of Ministers to the Member States on measures against sound and audiovisual piracy.

which are modified or altered in order to restrict its access to a specific audience". The Council of Europe emphasizes in the explanatory memorandum that the definition (and, by the same token, the protection arising therefrom) applies to all organizations offering encrypted services, whether at local, regional, national or transnational level, irrespective of the country of origin of the broadcast.

The protection guaranteed by the Council of Europe is not subject to the requirement of reciprocity. As the Council of Europe emphasizes in the explanatory memorandum, non-application to services originating from other countries could well give rise to problems for services originating from the country of reception.

The Recommendation defines *decoding equipment* as "any device, apparatus or equipment designed or specially adapted, totally or partially, to enable access in the clear to an encrypted service, that is to say without the modification or alteration of its characteristics".[20]

Finally, *distribution* is defined as the sale, rental or commercial installation of decoding equipment, as well as the possession of decoding equipment with a view to carrying out those activities. This covers commercial, not private activities.

The Recommendation urges Member States to provide for criminal or administrative *sanctions* in respect of all of the above-mentioned activities, with one exception. The marketing and advertising of the manufacture, importation or distribution of unlawful equipment does not give rise to criminal or administrative sanctions.[21]

The *civil remedies* proposed in the Recommendation provide that, in addition to the criminal sanctions, the injured encrypting organization should be able to take action against those involved in unlawful activities to obtain damages, or a share of the profits.

There are no rights of action for the rights owners of programmes included in the services. The Council's view, as expressed in the explanatory memorandum, is that although holders of the rights in broadcast programmes may suffer if illicit access occurs, this damage is indirect. The explanatory memorandum also states that a rights holder can ensure its interests are protected contractually by requiring the broadcaster to take legal action against illicit access.[22]

---

[20] As stated by the Council of Europe in the explanatory memorandum, the principles of the Recommendation are to apply exclusively to the part of the decoder that enables the signal to be decrypted. Thus, in the case of a system using smart cards, the part covered would be the card only and not the decoder as such since the latter cannot, on its own, decrypt the signal.

[21] The Council of Europe justifies the exception on the grounds that sanctions should be aimed exclusively at manufacturers, importers and distributors of unlawful decoding equipment, and not at organizations that simply carry material used for commercial promotion or advertising (advertising agencies, newspapers and magazines).

[22] While it is true that rightholders may include such clauses in contracts, this does not obviate the need to protect interests specific to the rights holder independently of those of broadcasters. When the unlawful activity affects the rights holder and not the broadcaster the broadcaster may have little incentive to act swiftly against those activities. Admittedly, the rights holder could take legal

Finally, the Recommendation does not provide for any sanctions, either civil or criminal, in respect of private possession of unlawful equipment.

The Recommendation has played a major role in the regulatory movement at Member State level that began in the early 1990s: specific national regulations on the legal protection of encrypted broadcasting services introduced at the time have often been inspired by the principles enshrined in the Recommendation.

However, in view of the very nature of the text, which is not binding, there are substantial differences between regulations, in particular with regard to scope, unlawful activities and the level of sanctions. Moreover, a number of Member States have not yet transposed the principles of the Recommendation into national law, thus giving rise to the present regulatory fragmentation at European level.

2. The World Intellectual Property Organization (WIPO) Study

In the context of the current talks on the draft Protocol to the Berne Convention and on the New Instrument for the protection of the rights of performers and producers of phonograms, the draft memorandum drawn up by the International Bureau in April 1994[23] suggests, in Chapter IX "Enforcement of rights", looking into the possibility of including measures against the abuse of technical devices.

It is suggested, in the context of those provisions, that the manufacture, importation and distribution, for sale or rental, of any device enabling or assisting the reception of an encrypted program broadcast or otherwise communicated to the public, by those who are not entitled to receive it should rank as breaches of copyright.

Moreover, the rightholders of a programme decrypted by means of an unlawful decoding device would be able to take legal action to obtain compensation.

Since the talks are still under way, it is too soon to say whether these proposals will be included in the final text. However, if they are included, the scope would not be limited to broadcasting but would cover any form of "communication to the public" of the protected work.

---

action against the broadcaster to enforce the original contractual provisions, but this acts as a further delay in the action against the pirate.

[23] Doc. WIPO 9099D/COP/0691D of 29 April 1994.

Chapter 3: Member States' legislation

1. Overview

The analysis of the regulatory environment focuses on the solutions provided by national legislations to the problem of *illicit reception of an encrypted service*, i.e. reception, without payment and/or authorisation, by persons not authorised by the service provider.

A succinct analysis of the regulatory solutions of each Member State to the problem of illicit reception of encrypted services is set out below. It should however be noted that the legislative environment can evolve very rapidly and any "snapshot" could cease to be relevant within a very short time.

2. Regulatory environment in the Member States (summary)

A single systematic approach to the problems raised by illicit reception of encrypted services does not currently exist in Europe. In certain countries, there are, in fact, *specific regulations*, others resort to *existing provisions*, while some do not have *any legal protection*.

In this respect it should also be noted that although the "cable and satellite" Directive[24] has harmonised the treatment of protected works used in satellite broadcasting and the management of cable retransmission within the Community, it does not in any way assist operators in their fight against illicit reception.

Indeed right holders could, under certain conditions, prohibit the unauthorised retransmission of their works but not unauthorised reception. This is because the latter does not consitute a relevant "act" for the purposes of copyright which covers traditionally communication and does not cover the reception of a protected work. Consequently, the national regulations implementing the Directive will not be of any use in preventing illicit reception of encrypted services.

Table I: Legislation on the protection of encrypted services

	Specific legislation				General legislation	
	Broadcasting	Telecommunications	Intellectual property	Criminal law	Unfair competition	Intellectual property
Austria					x	
Belgium		x			x	
Denmark						
Finland		x				
France	x			x		
Germany					x	
Greece						
Ireland	x					
Italy	x					
Luxembourg						
Netherlands				x	x	
Portugal						
Spain						x
Sweden				x		
United Kingdom	x		x			

[24] Directive 93/83/CEE mentioned above.

2.1 Application of provisions on unfair competition and Intellectual Property

Countries which do not have any specific rules on this subject often make use of other *more general legislation*, in particular that of *unfair competition*, which protects against dishonest trade practices. The application of these principles has in some cases paved the way for a ban on the manufacture, importation and marketing (sale, rental or possession for commercial purposes) of unauthorised decoding devices (A, B, D and NL).

Generally, this has been based on the fact that unauthorised manufacturing and marketing of decoding devices deprive the encryptor of the *remuneration* normally payable in respect of the service provided. Unauthorised manufacturers would in effect be paid for a service that was being provided by someone else.

It has been recognized in some cases that there is competition between encryptors and manufacturers of illegal decoders, a precondition for applying the rules on unfair competition.[25] For this to apply, the party concerned must in effect be present on the market. The principles of unfair competition would not apply in the absence of a commercial interest which needs protection.

Moreover, an action based on unfair competition laws can normally be brought only in respect of the distribution and marketing of unauthorised decoding devices, not against their importation or possession. This means that it is difficult to start an action before the devices have actually been marketed or to request preventive measures.

Other general rules have proved unwieldy. Admittedly, in cases of unauthorised manufacture of decoding devices, industrial property law already gives rightholders some protection. Several components of the device will indeed be covered by industrial property or intellectual property rights.

However, such action has often proved ineffective. On the one hand, in order to prove that a smart card contains a copy of the system owners software, the encryption algorithm, and by the same token the technology used, will have to be disclosed in the course of the proceedings, thus opening the door to further copying. On the other hand, proceedings based on the industrial property contained in the card would prove pointless in the case of genuine cards fraudulently reactivated after their period of validity had expired.

Such a course of action is in any case not always open to encryptors since they do not hold the industrial property rights concerned and cannot, therefore, institute proceedings against manufacturers of unlawful devices.

2.2 Application of specific regulations

Specific legislation on the protection of encrypted services against illicit access is a fairly recent phenomenon, resulting from the technological development seen in the

[25] In this respect, an Austrian Court of Appeal recognised explicitly (Case Teleclub v Olbort) that actual competition between parties is not required, where the goods are, by their nature, already competitive.

communication sector in the late 1970s. Following the wave of illicit decoding devices that flooded the market in countries where encrypted broadcasting was most developed (F, UK), the first regulations were adopted in 1987 in France and in 1988 in the UK.

A second wave of legislation took place in the early 1990s, as encrypted stations spread across Europe, viz. the legislation adopted in Ireland, Belgium (1991), Italy (1992), Finland and Sweden (1994). This process is not yet over, as shown by the debate in Denmark concerning the presentation of a draft law.

Where it exists, the legislation has traditionally been in the form of a *specific audiovisual law* which, modelling itself on copyright rules, provides for criminal sanctions for certain activities relating to the illicit reception of encrypted services and gives operators, and in some cases other interested parties, the right to claim damages from those responsible for such activities.

Accordingly, the situation with regard to current national regulations on the protection of encrypted services can be summarised up as follows:

2.2.1 Objective of the measures: protecting encrypted services against illicit reception

Although the national regulations concerned do not all have the same definition of illicit reception - this is sometimes referred to as *receiving pay-television programmes without paying the fee* (B, F, UK) or *access to an encrypted system without the encryptor's authorisation* (S, I) - the objective is invariably the same: *to ensure that only authorised people can receive the service*.

There is, however, a *division* between legislation which covers *only broadcasting and cable distribution services*, i.e. where the same programme is communicated to the public at large (I, F, B, IRL, S) and legislation that also covers *information services which are carried on networks and function on individual demand* (SF, UK, NL); the latter makes no distinction between services communicated to the general public and services sent on demand.

Where legal protection against illicit reception of an encrypted broadcasting service is available, it normally protects every type of broadcasting signal, whereas this is not always the case for radio services. However, some Member States (UK, IRL) grant such protection on the basis of the *origin* (national or foreign) or *of how the service is broadcast* (by satellite or terrestrial).

Table II: Types of protected services

Protected signals	Broadcasting			Radio	Other	Against pay only
	Cable	Satellite	Other			
Austria						
Belgium	x	x	x			x
Denmark						
Finland	x	x	x	x	x	
France	x	x	x			x
Germany						
Greece						
Ireland	x					x
Italy	x	x	x	x		
Luxembourg						
Netherlands	x	x	x	x	x	x
Portugal						
Spain						
Sweden	x	x	x	x		x
United Kingdom	x	Only for services originating in the UK	x	x	x	x

National legislation has followed *two approaches* to protect service providers against reception by unauthorised persons.

The first consists in *protecting the encrypted signal*. This is normally done by recognising the encryptor's *right of ownership in respect of the signal*. The unauthorised reception of the encrypted signal is therefore regarded as "theft", against which the owner has a right to be protected (B (French Community), IRL, I, UK, NL, SF). As a secondary effect, legislation of this type sometimes prohibits retransmission, interception and activities related thereto, in so far as they facilitate and/or allow illicit reception of the signal.

Table III. Types of action

Encrypted television services	Interception	Use	Transmission	Organise/allow reception by third parties
Austria				
Belgium*	x		x	x
Denmark				
Finland		x		
France		x	x	x
Germany				
Greece				
Ireland	x			x
Italy	x		x	
Luxembourg				
Netherlands		x		
Portugal				
Spain				
Sweden				x
United Kingdom	x	x		x

* *French-speaking Community only*

The second approach consists in focusing directly on the need to prohibit *preparatory activities* (B (Flemish Community), F and S). Unauthorised reception as such will thus no longer be regarded as an unlawful activity, but the *commercial activities facilitating it* would nevertheless be prohibited.

Such a difference of approach impacts on the extent of the protection. As a rule, legislation based on the protection of signals against theft prohibits all preparatory

activities, be they for commercial or for private purposes. Those, however, that deal exclusively with the preparatory activities do not cover the behaviour of individuals.

Table IV. Purpose of unlawful activities concerning decoding devices

	Commercial	Non-commercial
Austria		
Belgium	x	x
Denmark		
Finland	x	x
France	x	x
Germany		
Greece		
Ireland	x	x
Italy	x	
Luxembourg		
Netherlands	x	x
Portugal		
Spain		
Sweden	x	
United Kingdom	x	x

Depending on the circumstances, the preparatory activities, which may either be an ancillary target of the ban on reception or be the specific subject of the legislation, can be placed under the following headings:

(a) *Manufacture of decoding devices* intended to enable reception of an encrypted service without payment of the subscription fee.

To ensure that private individuals can only receive the programme by means of the equipment manufactured directly by the encryptor or on his behalf, all the regulations concerned prohibit the manufacture of devices intended solely to enable reception of an encrypted service without payment of the subscription fee (B, F, I, S, SF, NL, UK and IRL);

(b) *Importation of decoding devices* intended to enable reception of an encrypted service without payment of the subscription fee.

With the gradual elimination of border controls there is undoubtedly a greater risk that unauthorised devices manufactured in a Member State which does not prohibit their manufacture might subsequently be imported for the purpose of enabling reception of an encrypted service without payment of any charge. The laws of some Member States (B, F, I, UK, SF and IRL) accordingly prohibit the importation of decoding devices designed to enable reception of an encrypted service without payment of the subscription fee;

(c) *Distribution of decoding devices* intended to enable reception of an encrypted service without payment of the subcription fee.

The activity which constitutes, however, the most serious threat to encrypted service providers is without doubt the marketing of equipment intended to enable reception of their service without payment of the subscription fee. To guard against this possibility, national legislation normally prohibits the distribution of decoding devices designed to enable reception of an encrypted service without payment of the subscription fee (B, F, I, S, UK, IRL, SF and NL);

(d) *Possession, for commercial purposes,* of decoding devices intended to enable reception of an encrypted service without payment of the subscription fee.

Possession for commercial purposes, in particular with a view to sale and/or rental, is another stage in the sequence of fraudulent activity leading to reception of an encrypted service without payment of the subscription fee; that is why some regulations (B, F, I, IRL, SF and NL) prohibit the possession, for commercial purposes, of decoding devices intended to enable reception of an encrypted service without payment of the subscription fee;

(e) *Possession, for private use,* of decoding devices intended to enable reception of encrypted service without payment of the subscription fee.

Although possession, for private use, of decoding devices intended to enable access to an encrypted service without payment of the subscription fee is intrinsically a less serious activity than possession for commercial purposes, some Member States (UK, NL, B, F and IRL) have taken the view that even the private possession of an unauthorised device should be prohibited;

(f) *Marketing* of decoding devices intended to enable reception of an encrypted service without payment of the subscription fee.

Where there are rules aimed at protecting the service provider against illicit reception, the laws of some Member States (B, F, UK, I, NL and IRL) also prohibit marketing activities for devices intended to enable reception of encrypted services without payment of the subscription fee;

Table V. Unlawful activities concerning decoding devices

Decoding devices	Manufacture	Importation	Distribution	Marketing and advertising	Possession for commercial purposes	Possession for private use
Austria						
Belgium*	x	x	x	x	x	x
Denmark						
Finland	x	x	x		x	x
France	x	x	x	x	x	x
Germany						
Greece						
Ireland	x	x	x	x	x	x
Italy	x	x	x	x	x	x
Luxembourg						
Netherlands	x		x	x	x	x
Portugal						
Spain						
Sweden	x		x			
United Kingdom	x	x	x	x		

*Flemish Community only

Most Member States also prohibit other ancillary activities, all of which are connected with the marketing of decoding devices.

Table VI. Other unlawful activities concerning decoding devices

Decoding devices	Adapt	Sell	Rent	Install	Maintain	Use	Buy	Other
Austria								
Belgium		x	x	x			x	
Denmark								
Finland						x		
France		x		x			x	
Germany								
Greece								
Ireland				x	x			
Italy		x	x					
Luxembourg								
Netherlands								
Portugal								
Spain								
Sweden		x	x	x	x			
United Kingdom		x	x					

*2.2.2 Sanction*s

National regulations generally provide for *criminal or administrative sanctions* if the law is broken, as well as the possibility of civil proceedings to obtain *damages and interest*. On the latter point there are several possible scenarios.

In the first case, no reference is made in the specific regulation to an action for damages and interest, which would normally mean that general principles should be applied (B, F, I and NL).

In the second case, there may be a specific reference to rules covering actions for damages and interest (such as the Danish draft law). The explanatory memorandum to the draft Law states that both service providers and right holders of a broadcast should be able to claim damages and interest for the losses caused by the activities of unauthorised manufacturers.

The third possibility is that of a provision that applies the civil remedies of copyright holders (UK). This includes the possibility of obtaining cessation of the fraudulent activity and the indemnisation of damages and interest. The final possibility is that of a provision containing specific civil remedies, that states who may bring proceedings and the possible types of actions (IRL).

Table VII. Sanctions

Sanctions	Fine	Prison sentence	Administrative provisions	Civil provisions
Austria				
Belgium	BFR 26 to 100 000 (ECU 0.7 to 650)		Confiscation of decoding equipment, forfeiture of profits	
Denmark				
Finland	fine	up to two years	Seizure of equipment, forfeiture of profit	
France	FF 5 000 to 200 000 (ECU 772 to 30 880)	up to two years	Seizure of the technical information, seizure and confiscation of devices and advertising material, forfeiture of profit	
Germany				
Greece				
Ireland	up to IRL 20 000 (ECU 24 554)	up to two years	Seizure and forfeiture of equipment used in the commission of the offence	Specific remedies
Italy	LIT 500 000 to 6 million (ECU 220 to 2 645)	3 months - 3 years		
Luxembourg				
Netherlands	up to HFL 100 000 (ECU 48 670)	up to three years	Forfeiture of goods, forfeiture of profit	
Portugal				
Spain				
Sweden	fine	up to six months	Seizure of objects and equipment used in the commission of the offence, forfeiture of profit	
United Kingdom	up to UKL 5 000 (ECU 6 045)	up to two years	Copyright remedies	Proceedings under copyright law

2.2.3 Disparities between measures

From the above, it is clear that there are major disparities between existing legislation, in particular as regards:

- scope (domestic services or services originating in other Member States; broadcasting services or any encrypted service, including services on individual demand);
- the degree of protection (ban on possession for private use and on marketing);
- the person who may bring proceedings for civil remedies (encryptor or any party concerned);
- the level of sanctions.

These disparities are even more marked in the absence of specific legislation.

Conclusion

In the late 1980s some Member States began to adopt specific legislation aimed at protecting encrypted services against illicit reception by means of unauthorised decoding devices. In order to provide the same protection, other Member States apply existing general legislative provisions that are already included in their legislation

(unfair competition, intellectual property laws). And yet another group of Member States provide no such protection at present.

This means that there are disparities between the legal treatment of the illicit reception of an encrypted service in the European Union: some activities may be prohibited in some Member States but be legal in others.

Q 1: The Commission would like to have any additional information to enable it to examine national regulations in greater detail.

CHAPTER 4: BARRIERS TO THE EFFICIENT OPERATION OF THE INTERNAL MARKET

In view of the regulatory environment in the Member States, the Commission considers that the present legislative differencies can create obstacles to the free movement of goods and services and can thus damage *the efficient operation of the Internal Market.*

Some of these obstacles seem incompatible with the principles of the Treaty and will therefore have to be removed. This applies, first, to certain national regulations which make a distinction, for the purposes of legal protection against illicit reception, *based on the origin of the service*. Under such rules, services originating from other Member States are sometimes protected against illicit reception only if the national authority has first issued a *certificate which entitles them to such protection*.[26]

Secondly, other regulations simply make it impossible for some services to obtain protection, because of *the means of transmission used*, e.g. when only hertzian services or services carried by cables are protected against illicit reception, whereas encrypted satellite services, all of which are of foreign origin, do not enjoy such protection.[27]This is consequently disguised discrimination.

In these cases the transfrontier provision of services, such as that which exists between the subscriber and the encryptor, would be rendered more difficult than the provision of national services. The latter would be automatically protected, whereas services originating from other Member States would not be so protected or would have to obtain prior authorisation in order to enjoy such protection. These measures do not seem justifiable in the light of European Court of Justice case-law. Indeed discriminatory measures affecting the freedom to provide services are compatible with Community law only if they can be brought within an express derogation, such as that contained in Article 56 of the Treaty, which refers to grounds of public policy, public security or public health.[28] In these particular cases, it would appear that none of the grounds in question could justify such discrimination. In this regard, *the Commission may put an end to such discrimination as part of its monitoring of the application of Community law*.

By contrast, the analysis of national regulations has identified a number *of obstacles to the free movement of goods and services which might be justified by a public interest objective, and therefore compatible with the principles of the Treaty*. For these obstacles, *an initiative to ensure the operation of the Internal Market might be necessary.*

1. Obstacles to the free movement of decoding devices (Article 30 *et seq.*)

---

26 See British regulations.

27 See Irish regulations.

28 Case C-288/89 "Mediawet" [1991] ECR I-4007.

Article 30 of the Treaty states that quantitative restrictions on imports and all measures having equivalent effect shall be prohibited between Member States.[29] *Manufacturing and marketing prohibitions* are indistinctly applicable regulations[30] which have *restrictive effects* on trade, in so far as they erect barriers to the importation and marketing of products originating in other Member States.

In the light of the case-law of the Court, these prohibitions are justified because they pursue public interest objectives. First, they aim to *protect the encryptor against those who might fraudulently profit from his activities* (namely manufacturers and distributors of unauthorised decoding devices), and to *protect the consumer* against the marketing of devices which, as they are not official, would no longer guarantee reception of the service if the operator were to change the system. This objective, which aims to ensure that trade is conducted within a framework of equity and fairness, is one of the general or public interest objectives which, according to the Court, may justify an obstacle to the free movement of goods. *The protection of consumers and the fairness of commercial transactions* have on several occasions

---

[29] In this context it should be remembered that the Court of Justice traditionally defines quantitative restrictions as prohibitions or limits on imports, and measures having equivalent effect to quantitative restrictions as "all trading rules enacted by Member States which are capable of hindering, directly or indirectly, actually or potentially, intra-Community trade" (Case 8/74 Procureur du Roi v Benoît and Gustave Dassonville [1974] ECR 837).

However, within this last category the Court makes a distinction. On one side, it places trading rules which constitute measures having equivalent effect to quantitative restrictions and are incompatible with Article 30 since they impose conditions applicable solely to imported products or make their sale or use more difficult or costly than the disposal of domestic production (measures that are applied distinctly). Where such measures, like quantitative restrictions, are discriminatory, they may, according to the Court, be justified only on the basis of the grounds listed in Article 36.

On the other side, as regards trading rules which have identical effects on imported and domestic products, the Court has stated that, even if they are equally applicable to domestic and imported products (measures that are indistinctly applied), these national rules may not create barriers to a product lawfully produced and/or marketed in another Member State unless they are necessary to satisfy mandatory requirements (in which the Court includes, in addition to the grounds of public interest listed in Article 36, public health, consumer or environmental protection, the fairness of commercial transactions, etc.) (Case 120/78 "Cassis de Dijon" [1979] ECR 649; Case 216/84 Commission of the European Communities v French Republic [1988] ECR 793).

In this case, obstacles to the free movement of goods resulting from disparities between the national laws will be justified where there is a direct link between the laws and the mandatory requirement (causality criterion), where the laws are appropriate and not excessive in relation to the requirement (proportionality criterion), where there is no equivalent legislation in the country of origin, and where there are no alternative solutions which would enable the objective to be attained while creating less disturbance for trade flows (substitution criterion).

Consequently, even though a national law is applicable without distinction, it could still be a measure having equivalent effect when the restrictive effects it entails on intra-Community trade, though justified by a mandatory requirement, go beyond what is necessary for the attainment of the result.

[30] They do not have the effect of favouring domestic production and entail the same restrictions for both domestic and imported products.

been recognized by the Court as justification for barriers to the free movement of goods.[31]

Secondly, these prohibitions aim to ensure the right to remuneration of the *intellectual property right holders* of encrypted broadcasts and *industrial and intellectual property* right holders in respect of devices.[32] However, the objective of ensuring the right to legitimate remuneration, whether it is the remuneration of the right holders for programmes or that of the right holders for the technology contained in unauthorised devices, is one of the rights which, under the case-law of the ECJ, is the specific aim of *industrial and intellectual property*.[33]

These rules also respect the *proportionality criterion*, since they confine themselves to prohibiting the marketing of devices manufactured without the prior authorisation of the encryptor, irrespective of their domestic or foreign origins; therefore they do not go beyond what is necessary for the attainment of the objective.[34] Finally, they also respect the *substitution and equivalence criterion*, since there are no alternative and less restrictive measures that would ensure the desired protection.

In conclusion, an obstacle to the free movement of decoding devices manufactured and marketed in the State of origin, without the prior consent of the encryptor, may be justified by consumer protection and the fairness of commercial transactions, as well as by the protection of industrial or intellectual property.

2. Obstacles to the free movement of services relating to decoding devices (Article 59 *et seq*.)

The analysis of national regulations has shown that some laws prohibit activities which are ancillary to the manufacture and marketing of illicit decoding devices. This applies to regulations which prohibit *the marketing, installation, maintenance and replacement of illicit decoding devices*.

These activities constitute the provision of services within the meaning of Articles 59 and 60 of the Treaty. Although these prohibitions are indistinctly applicable, they nevertheless do have restrictive effects on the free movement of services. Marketing

---

[31] Case 22/71 "Bequelin" [1971] ECR 970:; Case 58/80 Dansk Supermarked a/s v a/s Immerco [1981] ECR 181.

[32] This is why some national regulations refer to copyright provisions. Indeed they give the parties concerned (normally the encryptors) the same rights as are given to the right holders of a work protected against an unauthorised copy of the work itself. In both cases, the unauthorised copy, whether of a work or of a decoding device which permits reception of a service, deprives the right holder, or the supplier, of his legitimate remuneration.

[33] Case 78/70 "Deutsche Grammophon" [1971] ECR 502.

[34] By contrast, if the prohibitions in question were applied to the import and marketing of devices manufactured and marketed in the Member State of origin *with the consent of the encryptor*, they would be liable to result in economic barriers which would be disproportionate to the objective, and therefore incompatible with the principles on the free movement of goods as interpreted by the Court.

activities and/or after-sales services carried out by service providers established in other Member States would be prohibited.

Nevertheless, according to the case-law of the Court,[35] these restrictive effects may be justified; in fact these laws pursue public interest objectives such as the *protection of consumers*[36] and *industrial and intellectual property*.[37] In addition, these restrictive effects do not go beyond what is necessary for the attainment of the objective, and may therefore be regarded as proportionate.[38]

In conclusion, prohibitions on the marketing, installation, maintenance and replacement of decoding devices manufactured and marketed in the State of origin without the prior consent of the encryptor may be justified by the need to protect consumers and industrial and intellectual property.

3. Obstacles to the free movement of encrypted services

Obstacles to the free movement of encrypted services may also result from *the absence of legal protection in certain receiving States*. The consultation conducted by the Commission has confirmed that operators consider effective legal protection against illicit reception of the service to be an important factor when deciding whether to distribute the service in a country. The absence of such legal protection *certainly makes marketing more difficult and more haphazard*. Operators will have to bear additional costs due not only to the use of a particularly secure system, but also to the need to adopt particularly costly distribution systems for the decoding devices (normally rental).

---

35 The ECJ has drawn a distinction between discriminatory restrictions and those applicable without discrimination. The former could be justified by one of the grounds listed in Article 56 (public policy, public security or public health). However, with regard to measures which would result in restrictions which are applicable without discrimination, the ECJ has held that Article 59 requires not only the elimination of all discrimination against a service provider on the grounds of his nationality, but also "the abolition of any restriction, even if it applies without distinction to national providers of services and to those of other Member States, when it is liable to prohibit or otherwise impede the activities of a provider of services established in another Member State where he lawfully provides similar services". (Case 76/90 Manfred Säger v Dennemeyer and Co. Ltd [1991] ECR I-4221). According to the Court it follows that a prohibition, which is applicable without discrimination could nevertheless constitute a restriction on the freedom to provide services insofar as it established obstacles which were not justified by overriding reasons relating to the public interest, insofar as that interest is not already protected by the rules to which the services provider is subject in the State of establishment, and insofar as the same result cannot be obtained by less restrictive rules. The Court includes among these overriding reasons relating to the public interest the protection of consumers and workers, industrial and commercial property etc.

36 Case 220/83 Commission v France [1986] ECR 3663.

37 Case 62/79 Coditel [1980] ECR 881.

38 The solution would probably be different in the case of devices manufactured and marketed in the State of origin *with the consent of the encryptor*. In this case, these restrictions would in fact create barriers to trade between Member States which were disproportionate in relation to the objectives to be achieved, and therefore incompatible with the principles of the Treaty on the freedom to provide services, as interpreted by the Court.

A legal void of this kind gives rise to *restrictive effects* on the movement of encrypted services in the Internal Market, since their distribution in countries without legal protection against illicit reception is made more difficult.

However, this restrictive effect is not contrary to Community law because, as has been recognized by the Court,[39] in the absence of any Community harmonisation, Member State are free to regulate economic activities in their territory in line with the principles of the Treaty. They may therefore decide, whilst respecting the proportionality criterion, whether or not to prohibit certain activities on the grounds of general interest objectives.

In conclusion, regulatory policy considerations relating to economic activities, which are for the Member State to assess, may justify the restrictive effect entailed by the regulatory void in the absence of any Community harmonisation.

4. Distortions of competition

Disparities between national regulations or the absence of such regulations in some Member States may also lead to *distortions of competition* in the Internal Market. An operator who distributes his decoding devices in a State with strong legal protection will have competitive advantages (which will for example be reflected in his programme purchasing capacity) over the operator who has to distribute his service in a State without effective legal protection, since the latter will have to bear additional costs resulting for example from the choice of a particularly secure distribution system.

This disparity between the competitive environments of the Member States could have adverse consequences for the development of encrypted services in the Internal Market, since operators would not be subject to the same market conditions within the European Union.

In conclusion, disparity between regulations may lead to distortions of competition which might make it more difficult to develop encrypted services.

Q 2: The Commission would like to know the opinion of the parties concerned on the existence of restrictions and restrictive effects other than those identified above.

[39] Case 52/79 Procureur du Roi v Marc J. V. C. Debauve and Others [1980] ECR 833.

CHAPTER 5: THE NEED FOR AND POTENTIAL TYPES OF COMMUNITY ACTION

The preceding analysis demonstrates that there are a number of *obstacles to the efficient operation of the Internal Market*; some of these obstacles may prove to be *incompatible with Community law* and would have therefore to be removed. This would apply to those obstacles caused by the application of national legislation which on the grounds of protecting encrypted services, make a distinction between the *nature* (hertzian or by satellite) or the *origin of the service*.

Other obstacles could however be *justified by general interest objectives such as the protection of consumers, and intellectual and industrial property rights where they respect the principle of proportionality.* This applies to obstacles to the free movement of decoding devices and other services linked to them flowing from the disparity in national regulations relating to the manufacture and marketing of these decoding devices.

Furthermore, from an economic point of view, consultations have shown that the current differences between regulatory solutions together with the additional costs and legal insecurities which they cause, are peceived by the market leaders as *a major impedement to the development of new encrypted services.* Effective legal protection against illicit reception is a fundamental factor in persuading an investor to develop an encrypted service and to launch it in other Member States.

Consequently, in respect of this last type of obstacles, *an action to establish an equivalent level of protection amongst all the Member States could prove necessary to eliminate the obstacles identified and to complete the regulatory framework for the European audiovisual sector established by the "Television without frontiers" Directive (89/552/EC) and the "Cable and satellite"Directive (93/83/EC) .*

In this respect it should be emphasised that insofar as the objective sought is *the removal of obstacles to the efficient operation of the Internal Market* caused by disparities between national regulations for the legal protection of encrypted services, such an objective may be attained solely through *Community harmonisation*. Indeed, it seems implausible that the Member States would spontaneously carry out a rapprochement of national regulations which concern the legal protection of encrypted services. However, should the case arise, the fact that it would not be within the institutional framework of the Community legal order would render it ineffective and fail to grant the industry the necessary legal security for the development of encrypted services.

However, before deciding in favour of a regulatory initiative, the Commission would like to know the opinion of the parties concerned on the initiatives which appear below.

1. Aim of the action

The general objective of the measure would be to enable media professionals, whether encrypted service providers, suppliers of programmes or manufacturers of devices, to benefit in full from the opportunities offered by the Internal Market. Indeed, in the perspective of the Information Society, there is a risk that the full potential of these

opportunities will not be realised if these companies do not enjoy sufficient legal protection within the Union.

A clear regulatory framework, which would secure, throughout the Community, legal *protection* against illicit reception of the service and would thus ensure the *free movement* of services and of goods is a necessary precondition for the development of the new services.

Moreover, considering the global nature of the problem of illicit reception, work should be launched on an international level, especially within the framework of bilateral agreements and the work of the WTO, in order to establish effective and efficent rules on a worldwide scale. Indeed, an initiative to establish a regulatory framework within the Internal Market would be incomplete if it did not include an external dimension aimed at resolving the problem on an international level and providing *protection against imports from third countries*.

2. Consistency with other Community policies

A regulatory initiative to ensure the legal protection of encrypted services would also be consistent *with other Community objectives and policies*.

- *A regulatory framework providing a high level of legal protection at Union level would help to develop the European encrypted services and decoding equipment manufacturing industries*. Without effective legal protection, illicit reception and the resulting loss of revenue could undermine the financial stability of encrypted service providers and make it more difficult to develop such services. Similar consequences would affect the decoding equipment manufacturing industry which, in the absence of legal protection, would not embark on an activity that was not protected against fraudulent actions.

- *A regulatory intervention to ensure the efficient operation of the Internal Market would be coherent with the objectives pursued by the audivisual and cultural policy of the Union*. Such a measure would ensure that greater advantage was taken of intellectual property rights for programmes broadcast by TV channels, which would lead to increased operating resources for *audiovisual production*. Indeed, the new encrypted services are important for the development and circulation of artistic creation, as well as for the growth of the Union's cultural and linguistic diversity; however, the right holders will be reluctant to assign their rights if encrypted services are not protected from illicit reception. If this means that encrypted services are deprived of programmes, they will be unable to develop, and audiovisual creation will have lost the opportunity of benefiting from a powerful broadcasting medium.

- *A regulatory intervention to ensure the operation of the Internal Market would be consistent with the objective of consumer protection*. In the absence of a secure regulatory framework, consumers could be mislead about the origin of the decoding device they are purchasing and thus believe they are buying authorised equipment, whereas it is in fact a

pirated decoder. In this case, if the operator modifies the encryption system for security reasons, the device purchased will be of no use to the consumer, who will have to pay for another decoder. Moreover, unauthorised devices will not always be guaranteed by the pirate manufacturers: should the device breakdown, the consumer will have to bear the cost of repairs. In both cases, there are clear disadvantages for the consumer from the marketing of unauthorised decoding devices. In addition, the losses suffered by the service providers have a negative effect on their financial stability; consequently, the development of encrypted services could be delayed by the lack of protection and this situation would represent a loss for the consumer, who would be unable to benefit from the service.

3. Choice of instrument and legal basis

In view of the analysis carried out, following consultation with the interested parties, the Commission could decide to adopt one of the following two measures.

The Commission could propose a *directive to harmonise national legislations* (Option 1). In this respect, whilst taking account of the principles of proportionality and subsidiarity, the proposed Directive could provide for minimal harmonisation leaving the Member States free to adopt stricter measures, which would ensure a *minimal level of equivalent protection* within the Union. This option would have the advantage of securing legal protection for the sector concerned whilst leaving the Member States some flexibility to widen the scope of this protection.

The Commission could, alternatively, propose a *Council regulation* (Option 2). This option would have the same objective as the option above and the advantage of securing a more effective harmonisation as it would be directly applicable in the Member States without being implemented by national law.

Moreover the chosen option could be accompanied by a proposal to modify the existing Community law provisions in respect of the free circulation of counterfeit goods originating from third countries,[40] so that the measures could apply with equal force to decoding devices. It should nevertheless be noted that this measure alone is inadequate to ensure effective legal protection within the Union. In effect, the regulatory measures applicable to counterfeit goods are based on a voluntary agreement by operators and interested parties, and apply solely to goods orginating from third countries when they are imported into the Union. Trade between Member States is regulated by national and Community regulations. However, there is no real uniformity between national regulatory approaches to the manufacture and marketing of illicit decoding devices ; this results in divergences between possible solutions and in some cases there is a lack of protection. It therefore follows that an intervention to control imports from third countries should accompany any regulatory proposal to ensure protection against illicit reception within the Union.

[40] Council Regulation (EC) N° 3295/94 of the Council (O.J.E.C L 341 of 30.12.1994) laying down measures to prohibit the release for free circulation, the export, re-export or entry for a suspensive procedure of counterfeit and pirated goods.

The appropriate legal basis would be Articles 57(2), 66 and 100a, taking into account the objective of ensuring the efficient operation of the Internal Market and of enabling the free movement of services and goods.[41]

4. Scope of application

The harmonisation envisaged would cover the *current national regulations in the field of the legal protection of encrypted services.* These regulations, where present, may be found in copyright law, broadcasting law, civil law or administrative law. Consequently their location in national law is unimportant; what counts is their objective, i.e. the protection of encrypted services against illicit access.

Such harmonisation could cover *all encrypted services*, for which *encryption is used to ensure the payment of a fee*, without being restricted to broadcasting services. This category would therefore include the *traditional encrypted broadcasting services* (cable, hertzian or satellite), the *new broadcasting services* (digital television, pay-per-view, near video on demand) and *Information Society services, namely services provided electronically at a distance on the individual demand of a service receiver* (video on demand, supply of games on demand, interactive teleshopping).

Indeed, where a service is encrypted to limit its reception, it will need the same protection independent of the type of service concerned (broadcasting, on individual demand etc.). On the other hand, if harmonisation were confined to broadcasting services alone, it would not be possible to cover the new uses of encryption such as data transmission on individual demand or without images (e.g. a newspaper sent to a home via satellite), as well as video games delivered directly to a home, by satellite or cable.

Consequently, *all encrypted services*, for which decoding devices are available to the public, *should be able to enjoy the same protection*. Looking ahead to the convergence of broadcasting and information technology services, the definition of "encrypted services" should cover any service which can be received by a television or computer screen, i.e. radio or television broadcasting services, as well as the other interactive Information Society services, which are defined in the proposal for a Directive on regulatory transparency in the Internal Market, namely distance services transmitted electronically on the demand of the service receiver.

However, harmonisation *should not cover* the services which use encryption for reasons other than that of ensuring payment of a fee, such as services which are encrypted to ensure *the integrity and confidentiality of the message transmitted*, namely financial or telecommunications services. The reason for this exclusion is that *the general interest objectives* put at risk if they are intercepted, i.e. the integrity and confidentiality of the communication, differ significantly from the protection of the value of a service provided in exchange for a fee, which is the general interest objective threatened by illicit reception. This difference has led to *regulatory solutions which differ significantly*, both at national and international level, in

[41] In the event that the counterfeit goods Regulation were to be amended, the legal basis would remain unchanged, i.e. Article 113.

particular as regards the action to be taken and the level of sanctions, and which do not justify joint treatment of the two problems.

Protection against goods from third countries should cover all decoding devices imported from a third country which enable reception of an encrypted service without the prior authorisation of the encryptor.

5. Overall structure

In view of the proportionality principle, the proposed provisions could prohibit the following activities:

- the manufacture of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the sale of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the possession for commercial purposes of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the possession for private purposes of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the installation, maintenance and replacement of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the marketing of decoding devices intended to permit access to encrypted services without the authorisation of the encryptor;

- the decoding of encrypted broadcasts without the authorisation of the encryptor.

The proposed measure should also provide that Member States adopt *effective, proportionate and deterrent penalties for the breach of these provisions*. In this respect, as the Commission has stated in its communication on the role of penalties in implementing Community legislation,[42] the Member States would remain free to determine the structure for these sanctions. The measure could therefore provide for a procedure whereby the Commission is notified of provisions which Member States intend to adopt.

It should also enable any interested party to bring a claim *for damages and interest*.

As regards provisions on protection against the release into circulation of goods from third countries, the proposed measure should prohibit the importation of decoding

[42] Communication from the Commission to the Council and the European Parliament on the role of penalties in implementing Community Internal Market legislation COM(95) 162 final of 3 May 1995.

devices intended to permit access to encrypted services without the authorisation of the encryptor.

Q 3: The Commission would like to know the opinion of the parties concerned on the need for harmonisation at Community level.

Q 4: The Commission would like to know the opinion of the parties concerned on the form of a possible harmonisation instrument from the options presented in the Green Paper.

Q 5: The Commission would like to know the opinion of the parties concerned on the content of a possible harmonisation instrument, as envisaged above, in particular:

i. the scope

a. should this be limited to broadcasting services or extended to all services in which encryption is used to ensure payment of the subscription fee;
b. if the scope were to be extended, would the criterion used be appropriate (services encrypted to ensure payment of the subscription fee), or should another criterion be used to determine the scope ? If so, would it be considered necessary for the harmonisation instrument to protect all services against illicit reception which use conditional access techniques, including for example passwords (whether they are encrypted or not)?

ii. the desirability of including the possession by private individuals of unauthorised decoding devices;

iii. claims for damages and interest.

LIST OF QUESTIONS

Q 1: The Commission would like to have any additional information to enable it to examine national regulations in greater detail.

Q 2: The Commission would like to know the opinion of the parties concerned on the existence of restrictions and restrictive effects other than those identified above.

Q 3: The Commission would like to know the opinion of the parties concerned on the need for harmonisation at Community level.

Q 4: The Commission would like to know the opinion of the parties concerned on the form of a possible harmonisation instrument from the options presented in the Green Paper.

Q 5: The Commission would like to know the opinion of the parties concerned on the content of a possible harmonisation instrument, as envisaged above, in particular:

i. the scope

a. should this be limited to broadcasting services or extended to all services in which encryption is used to ensure payment of the subscription fee;
b. if the scope were to be extended, would the criterion used be appropriate (services encrypted to ensure payment of the subscription fee), or should another criterion be used to determine the scope ? If so, would it be considered necessary for the harmonisation instrument to protect all services against illicit reception which use conditional access techniques, including for example passwords (whether they are encrypted or not)?

ii. the desirability of including the possession by private individuals of unauthorised decoding devices;

iii. claims for damages and interest.