



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, 24.04.2003
COM(2003) 198 final

PROTECTION JURIDIQUE DES SERVICES ELECTRONIQUES PAYANTS

Rapport de la Commission au Conseil, au Parlement européen et au Comité économique et social européen

sur la mise en œuvre de la directive 98/84/CE du Parlement européen et du Conseil, du 20 novembre 1998, concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel

Résumé

Ce premier rapport de la Commission sur la mise en œuvre de la directive 98/84/CE dont l'objectif est de fournir un niveau minimum de **protection juridique contre le piratage des services électroniques payants** (télévision à péage, radio et services internet) dans l'UE, fait partie de la stratégie globale du marché intérieur de la Commission visant à supprimer les entraves aux services. Il décrit et analyse les aspects marquants des principales dispositions de la directive, leur mise en œuvre et leur application par les États membres et les pays candidats ainsi que l'évolution actuelle du piratage. Il couvre la période qui va de novembre 1998 (adoption de la directive) à la fin de l'année 2002.

Le rapport estime que les économies basées sur la connaissance du 21^{ème} siècle devraient progressivement se fonder sur une généralisation des **services électroniques payants** et que le piratage des services électroniques payants aura les mêmes effets préjudiciables pour la société de la connaissance que la criminalité en col blanc et la contrefaçon de marchandises au vingtième siècle. La protection juridique contre le piratage de services électroniques payants est une importante **contribution à la réalisation de l'objectif ambitieux de l'Union de devenir l'économie la plus dynamique et la plus compétitive d'ici à 2010**.

Le rapport insiste sur le fait que le piratage résulte de l'impossibilité de capter des **chaînes de télévision par satellite d'autres États membres qui sont protégées**. Il note que les citoyens de l'UE ne parviennent pas à comprendre pourquoi, dans le marché intérieur, ils ne peuvent accéder légitimement aux services de télévision à péage protégés même s'ils sont prêts à payer. En conséquence, le rapport invite les acteurs du marché à rechercher activement des **solutions contractuelles** et signale que la Commission contribuera à ce processus dans le cadre de la révision de la directive concernant le droit d'auteur lié à la radiodiffusion par satellite et à la retransmission par câble.

Le rapport montre que la **mise en œuvre** de la directive n'a pas encore été totalement achevée dans l'Union élargie, que **l'application** au niveau national doit être consolidée et que des **efforts conjoints** contribueront à lutter efficacement contre le piratage. Il ne sera possible de lutter contre le piratage que si les pirates ne trouvent pas de sphères de sécurité en Europe. La Commission continuera donc à coopérer avec d'autres pays européens et les organisations internationales concernées afin de créer **un cadre juridique cohérent pan-européen contre le piratage de services électroniques payants**, en particulier par une entrée en vigueur rapide de la convention n° 178 du Conseil de l'Europe.

Le rapport observe que le **piratage de services électroniques payants est considéré comme un cyber-crime**. Il conclut qu'il serait **prématuré de proposer des modifications** de la directive mais que les consultations et évaluations faites dans le cadre du rapport ont déjà permis à la Commission d'identifier plusieurs thèmes qui méritent une réflexion plus approfondie, en étroite coopération avec les États membres et l'industrie. Parmi ces thèmes, on peut citer la nécessité d'un **cadre d'exécution équilibré et cohérent**, applicable à tous les types de piratage et de contrefaçon, approuvé au niveau communautaire, ainsi que la **vente de clés et de dispositifs illicites** par internet.

SOMMAIRE

1.	Introduction	4
2.	Contexte et contenu de la directive	4
2.1.	Contexte	4
2.2.	Dispositions clés de la directive	6
2.2.1.	définitions	7
2.2.2.	Activités illicites	8
2.2.3.	Sanctions et voies de droit	9
2.3.	Questions soulevées lors de l'adoption de la directive	9
2.3.1.	Utilisation d'un accès conditionnel pour des raisons autres que la rémunération du prestataire de service	9
2.3.2.	Objectifs commerciaux/objectifs privés	10
3.	Mise en œuvre de la directive	11
3.1.	Communication des mesures de mise en œuvre	11
3.2.	État actuel de la mise en œuvre par les États membres	11
3.3.	Dispositions nationales allant au delà des exigences de la directive	13
3.4.	Élargissement	14
4.	Évolutions du marché et application de la directive	15
4.1.	Consultation des acteurs du marché	15
4.2.	Combattre le pir@tage – une cible mouvante	16
4.3.	Assurer le respect	21
4.4.	Pratiques commerciales exposées au piratage	22
5.	Autres développements juridiques concernant la fourniture de services d'accès conditionnel	24
5.1.	L'adoption de la directive 2001/29/CE sur le droit d'auteur dans la société de l'information	24
5.2.	L'adoption d'un nouveau cadre réglementaire pour les services de communications électroniques	25
5.3.	La mise en œuvre de la directive 2000/31/CE sur le commerce électronique	26
5.4.	La proposition d'une décision-cadre du Conseil relative aux attaques visant les systèmes d'information	27
6.	Combattre le piratage – un effort pan-européen	28
6.1.	Recommandation n° R(91)14 sur la protection juridique des services de télévision cryptés	28
6.2.	Convention européenne STE n° 178 sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel	29
6.3.	La situation juridique dans les autres pays européens	29
6.4.	Convention européenne STE n° 185 sur la cybercriminalité	30
7.	conclusions et prochaines étapes	30
7.1.	Les services électroniques payants sont importants pour une économie basée sur la connaissance arrivant à maturité	30
7.2.	Renforcement de la protection juridique actuelle – actions à entreprendre	31
7.3.	Renforcer la protection juridique – et ensuite?	32

1. INTRODUCTION

Le présent document est le premier rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen sur la mise en œuvre de la directive 98/84/CE¹ concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel (ci-après dénommée "la directive").

L'objectif de cette directive est d'assurer, au sein de l'UE, un niveau minimum de protection juridique des services électroniques payants contre le piratage en interdisant toutes les activités de fabrication, de distribution et de vente, à des fins commerciales, de cartes à puces pirates et d'autres dispositifs permettant de contourner les systèmes de protection d'accès de services de TV à péage, de radio et d'internet.

L'article 7 de la directive prévoit que, au plus tard trois ans après l'entrée en vigueur de la directive² et, à compter de cette date, tous les deux ans, la Commission présente un rapport au Parlement européen, au Conseil et au Comité économique et social sur l'application de la directive, accompagné, le cas échéant, de propositions, en particulier en ce qui concerne les définitions de l'article 2, pour l'adapter en fonction de l'évolution économique et technique et des consultations menées par la Commission.

Le présent rapport traite de l'application de la directive depuis son adoption en novembre 1998 jusqu'à la fin de l'année 2002.

Le rapport décrit et analyse les aspects marquants des principales dispositions de la directive et leur mise en œuvre dans les législations nationales. Le rapport a été établi sur la base des informations relatives à la transposition fournies par les États membres, des avis exprimés par les acteurs du marché, en particulier sur le développement du piratage et les mesures prises par les autorités nationales, ainsi que des avis et analyses de la Commission. Il tient également compte des résultats d'une étude indépendante commandée en 1999 et qui traite de l'utilisation de l'accès conditionnel pour des raisons autres que la protection de la rémunération.

De plus, le présent rapport fait partie de la stratégie globale de la Commission pour le marché intérieur destinée à éliminer les entraves aux services³.

2. CONTEXTE ET CONTENU DE LA DIRECTIVE

2.1. Contexte

Les progrès technologiques, la libéralisation et l'harmonisation du cadre juridique ont conduit à une rapide multiplication des chaînes de diffusion radiophonique et

¹ JO L320 du 28.11.1998, p. 54; voir

http://europa.eu.int/comm/internal_market/fr/media/condac/dir/index.htm

² 28.11.1998

³ COM(2000)888final du 29.12.2000 "Stratégie pour le marché intérieur des services"; voir http://europa.eu.int/comm/internal_market/fr/services/services/index.htm

télévisuelle et les services de la société de l'information en Europe au cours de la dernière décennie du vingtième siècle. Ces nouveaux services sont principalement proposés par des sociétés commerciales et financés soit par les recettes publicitaires et la sponsoring, soit par le paiement de redevances et d'abonnements. Les stations de télévision à péage par satellite offrant des canaux à contenu de grande qualité (films) ou des canaux thématiques (sports, style de vie ou voyages) sont des exemples types de cette évolution.

Afin d'assurer la rémunération de leurs services, les prestataires utilisent ce que l'on appelle les techniques d'accès conditionnel qui, en principe, interdisent tout accès au service sous une forme intelligible sans l'autorisation préalable du prestataire de service. Tandis que le service protégé par un accès conditionnel peut faire l'objet d'une large réception, il ne peut être vu ou entendu que si le téléspectateur/l'auditeur utilise un décodeur spécial allant souvent de pair avec une carte à puce⁴ achetée auprès du prestataire de service. Cette méthode est très efficace en termes de garantie de paiement car seules les personnes ayant payé le dispositif - et que le prestataire de service cherche donc à atteindre - sont capables de décoder le service.

À l'heure actuelle, il existe environ 126 canaux de télévision transmis par satellite. La moitié d'entre eux sont cryptés par 12 systèmes différents d'accès conditionnel.

Satellite	Réseau	Système d'accès conditionnel	Principal marché
Astra	BSkyB	Videoguard	Royaume-Uni, Irlande
Astra	Canal Satellite Digital	Mediaguard	Espagne
Astra	CanalSatellite	Mediaguard; Viaccess	France
Astra	CanalDigitaal	Irdeto; Mediaguard	Pays-Bas
Astra	Première World	Betacrypt	Allemagne, Autriche
Astra	Wizja TV	Cryptoworks	Pologne
Astra	UPC Direct	Cryptoworks	Hongrie
Astra	UPC Direct	Cryptoworks	République tchèque; Slovaquie
Eutelsat	Tele+ Digitale	Mediaguard; Videoguard	Italie
Eutelsat	Absat	Viaccess	France, Belgique, Luxembourg
Eutelsat	TPS	Mediaguard; Viaccess	France
Eutelsat	Stream	Mediaguard; Videoguard	Italie
Eutelsat	Alpha Digital	Nagravision	Grèce; Chypre
Eutelsat	Nova	Irdeto	Grèce; Chypre
Eutelsat	Cyfra+	Mediaguard	Pologne
Eutelsat	Polsat	Nagravision	Pologne
Hispasat	TV Cabo	Nagravision	Portugal
Hispasat	Via Digital	Nagravision	Espagne
Sirius	Viasat	Viaccess	Scandinavie
Thor	Canal Digital	Conax	Scandinavie

tableau 1: principaux fournisseurs de TV payante par satellite en Europe (2002)

L'accès conditionnel comprend une série de technologies qui peuvent être - et qui, en pratique, sont - utilisées à des fins différentes. Outre la rémunération du service lui-même, l'accès conditionnel est également utilisé, souvent en parallèle, pour limiter l'audience potentielle à un territoire particulier, par exemple pour des raisons

⁴ Les cartes à puce sont des cartes plastiques de la taille d'une carte bancaire, comportant un microprocesseur et une mémoire et qui sont capables de traiter des données. En fait, les cartes à puce sont des ordinateurs de petite taille, portables et souvent sécurisés.

de droit d'auteur, ou à une catégorie particulière d'utilisateurs (exclusion des mineurs, par exemple).

L'arrivée de la télévision à péage a également marqué le début d'une industrie de piratage commerciale florissante. L'accès illicite à un service protégé par un accès conditionnel a plusieurs conséquences négatives pour les prestataires de services concernés. En les privant de leur rémunération, le piratage menace directement la viabilité économique de ces prestataires de services, la concurrence entre eux et, partant, la diversité des services offerts au public.

La technologie, seule, ne peut résoudre entièrement le problème du piratage⁵. Parallèlement aux contre-mesures techniques des prestataires de services, certains États membres ont introduit une nouvelle législation afin de combattre le piratage. D'autres ont tenté d'appliquer les dispositions existantes du droit pénal, de la législation contre la concurrence déloyale ou du droit de la responsabilité civile. Certains États membres n'ont aucune protection juridique. Une enquête de la Commission, effectuée durant l'année 1995⁶, a montré que la portée, les interdictions et les sanctions de la protection juridique accusaient des différences importantes d'un État membre à l'autre. Après avoir procédé à de très larges consultations, la Commission a proposé d'harmoniser la protection juridique de tous les services électroniques utilisant une quelconque forme d'accès conditionnel, afin de garantir la rémunération du service. La directive 98/84/CE⁷ a été adoptée à la fin de l'année 1998.

2.2. Dispositions clés de la directive

La directive a pour objectif de combattre le piratage de “services protégés” en interdisant les activités commerciales concernant les “dispositifs illicites”. Le principe de la protection juridique est de porter un coup d'arrêt à la vente “en amont” de décodeurs illégaux, c'est-à-dire d'empêcher que les utilisateurs finaux puissent acquérir des décodeurs illégaux et autres dispositifs connexes. Cette approche sera satisfaisante si les technologies et connaissances spécialisées nécessaires à la fabrication de cartes à puce et de décodeurs illégaux ne sont pas mises à la disposition des utilisateurs finaux intéressés.

La directive renforce également le fonctionnement du marché intérieur en refusant aux États membres la possibilité de restreindre la libre circulation de dispositifs d'accès conditionnel ou la libre fourniture de services à péage pour des raisons liées aux activités illicites de piratage spécifiées par la directive.

⁵ En 1991 déjà, le Conseil de l'Europe avait conclu qu'il était nécessaire de compléter la protection technique par des mesures juridiques appropriées; voir recommandation R(91)14 du Comité des ministres sur la protection juridique de services télévisuels cryptés;
<http://cm.coe.int/ta/rec/1991/91r14.htm>

⁶ COM(96)76final du 06.03.1996 – Livre vert sur la protection juridique de services cryptés dans le marché intérieur, voir http://europa.eu.int/comm/internal_market/fr/media/condac/dir/legproc_en.htm

⁷ La directive 98/84/CE ne garantit la protection juridique que des services d'accès conditionnel. La fourniture elle-même de ces services ainsi que les exigences techniques autorisant les dispositifs d'accès conditionnel font l'objet d'autres directives communautaires, comme par exemple la directive 2002/19/CE (directive "accès") et la directive 2002/22/CE (directive "service universel"); JO L108, du 24.04.2002;
http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

2.2.1. *définitions*

Service protégé

La directive couvre non seulement les services classiques de diffusion télévisuelle et radiophonique, mais également toute une gamme de services en ligne interactifs (services de la société de l'information⁸). La notion de « services » doit être entendue au sens de l'article 50 du traité (ex article 60)⁹, telle qu'interprétée par la Cour de Justice¹⁰. La directive protège les services à "contenu", quelles que soient les caractéristiques techniques du mode de transmission utilisé. Il s'agit de la première directive communautaire qui concerne à la fois les services de radiodiffusion télévisuelle et les services interactifs. On peut considérer que c'est la première fois qu'il est question de "convergence juridique"¹¹ dans un texte législatif communautaire.

Toutefois, pour pouvoir bénéficier de la protection prévue par la directive, il est nécessaire que les services utilisent une certaine forme d'accès conditionnel pour que le prestataire de service concerné perçoive une rémunération: il peut s'agir d'un abonnement (par exemple, pour pouvoir capter, au cours d'une période donnée, l'offre complète d'une chaîne particulière) ou du paiement d'un droit (par exemple, pour voir un film particulier). Ces paiements effectués directement au prestataire de service ont pour objectif de garantir la viabilité économique du service¹². Les modèles commerciaux permettant de fournir un service particulier contre paiement de la part du bénéficiaire, mais également des services secondaires sans paiement direct moyennant toutefois une protection de l'accès conditionnel, sont également couverts (par exemple les morceaux bonus ("bonus tracks") pouvant être téléchargés à partir d'internet par les propriétaires légitimes des CD audio originaux). Sans ce type de lien entre rémunération et service d'accès conditionnel protégé, la directive ne peut garantir aucune protection juridique.

La fourniture d'un accès conditionnel aux services radiophoniques, télévisuels et de la société de l'information - considérés dans la directive comme services à part entière - est également couverte par le concept de "service protégé". Si le prestataire

⁸ Les services de la Société de l'information sont définis à l'article 1(2) de la Directive 98/48/CE du Parlement Européen et du Conseil du 20 juillet 1998 portant modification de la Directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques.

⁹ Au sens de ce traité, sont considérées comme services les "prestations" fournies normalement contre rémunération, dans la mesure où elles ne sont pas régies par les dispositions relatives à la libre circulation des marchandises, des capitaux et des personnes.

¹⁰ Conformément à la jurisprudence de la Cour de justice, cette notion de service "fourni normalement contre rémunération" ne fait pas référence aux modalités concrètes du financement - l'article 60 (maintenant article 50 du traité UE) n'exige pas que le service soit payé par ceux qui en bénéficient (affaire C-352/85 Bond van Adverteerders [1988] REC 2085 §16) – mais à l'existence d'une contrepartie économique pour le service en question (affaire C-109/92 Wirth [1993] REC I-6447 §15).

¹¹ Progressivement, les techniques de communication et d'information utilisent les mêmes types (ou tout au moins des types similaires) de technologie (numérique). Cette "convergence technologique" touche de plus en plus les marchés et la fourniture de services dans le domaine de la diffusion, des services interactifs et des communications électroniques, et donc la réglementation concernée. Dans un tel environnement, où les frontières tendent à s'estomper, la "convergence juridique" grâce à la fusion d'instruments juridiques sur la base d'une approche commune, neutre sur le plan technologique, est souvent considérée comme le meilleur dispositif réglementaire.

¹² Voir considérant n° 6 de la directive.

de ce type de service n'a pas d'intérêt économique direct dans les services à "contenu" dont l'accès conditionnel est protégé, il a en revanche un intérêt économique immédiat à protéger la sécurité offerte par sa technologie d'accès conditionnel. Le piratage réussi de sa technologie de protection altère directement la confiance de ses clients dans sa capacité à protéger les services concernés et menace, par conséquent, sa viabilité économique.

Accès conditionnel

Le texte de la directive reste neutre à propos de la technologie. En ne mentionnant aucune technologie particulière, mais en utilisant des définitions fonctionnelles de haut niveau, la directive restera d'actualité et sera moins sujette à modification; de plus, elle fournit un cadre juridique plus stable et, par conséquent, une sécurité juridique optimale.

Cette directive couvre non seulement les technologies générales d'accès conditionnel basées sur le cryptage (comme par exemple pour la télévision à péage), mais également toute autre technologie interdisant l'accès au service sans l'approbation préalable du prestataire de service, tels que les systèmes d'identification de l'utilisateur/mot de passe souvent utilisés par les services payants fournis par l'intermédiaire d'internet.

Dispositifs illicites

Les dispositifs illicites doivent être conçus ou adaptés de manière à fournir un accès intelligible à un service protégé sans l'autorisation du prestataire de service. Parmi les exemples types de dispositifs illicites, on peut citer des matériels ou des programmes de logiciels spécifiques destinés à neutraliser la protection de l'accès conditionnel. Étant donné le développement des technologies concernant la carte à puce, des cartes à puce totalement fonctionnelles qui sont des cartes originales modifiées ou des duplicatas de cartes originales ou encore des cartes pirates totalement nouvelles sont, actuellement, les dispositifs illicites les plus répandus. Toutefois, les programmeurs de cartes à puce vierges ou standard¹³ ne sont pas considérés, en tant que tels, comme un dispositif illicite.

2.2.2. *Activités illicites*

Contrairement aux autres parties de la directive, les dispositions relatives aux activités illicites sont très normatives. La liste détaillée des activités à interdire couvre l'ensemble de la chaîne commerciale d'activités qui vont de la production initiale à l'entretien et à la réparation de dispositifs illicites, y compris toutes les formes de communications commerciales¹⁴.

La directive ne sanctionne que les activités commerciales¹⁵ favorisant une réception non autorisée et non pas la réception non autorisée en tant que telle. Elle traduit

¹³ Un programmeur de carte à puce est un équipement matériel connecté à un PC et contrôlé par lui, capable de charger des données dans la mémoire de la carte à puce.

¹⁴ Le considérant 14 explique ce que recouvre ce concept qui, au moment de l'adoption de la directive, n'existait pas encore dans le droit communautaire.

¹⁵ Le considérant 13 de la directive précise la notion de "à des fins commerciales" en faisant explicitement référence au "profit économique direct ou indirect".

clairement le principe qui consiste à stopper le piratage “en amont”, c'est-à-dire les activités permettant un accès illégal.

2.2.3. *Sanctions et voies de droit*

La directive n'oblige pas les États membres à imposer des sanctions spécifiques mais se contente de préciser que les sanctions doivent être effectives, dissuasives et proportionnées¹⁶. La directive ne fixe pas le niveau et le type¹⁷ des sanctions et ne porte pas atteinte à l'application de certaines dispositions du droit pénal national¹⁸.

Les États membres doivent mettre à la disposition des prestataires de “services protégés” une série de voies de droit appropriées, comprenant, au minimum, une action en dommages et intérêts, une mise en demeure ou autre mesure préventive ainsi que la possibilité, lorsque c'est approprié, de éliminer les dispositifs illicites des circuits commerciaux.

2.3. **Questions soulevées lors de l'adoption de la directive**

2.3.1. *Utilisation d'un accès conditionnel pour des raisons autres que la rémunération du prestataire de service*

Les techniques d'accès conditionnel contrôlent et sécurisent l'accès aux services à “contenu” transmis par voie électronique. Ces techniques permettent à leurs utilisateurs de déterminer les conditions précises d'octroi de l'accès.

La directive protège exclusivement les prestataires de services utilisant un accès conditionnel en vue de garantir leur rémunération. L'accès conditionnel peut, toutefois, servir à de nombreuses autres fins (ce qui est le cas dans la pratique). La plupart des systèmes d'accès conditionnel utilisés par les opérateurs de télévision à péage par satellite assurent le paiement mais ont également pour objectif de réduire l'audience potentielle de la diffusion à un territoire particulier (souvent un État membre), essentiellement pour des raisons de droit d'auteur. L'accès conditionnel est également utilisé pour protéger les mineurs contre des contenus contraires à la morale et réservés aux adultes.

Lors de l'adoption de la directive, la nécessité et la possibilité d'élargir la portée de la protection juridique offerte par la directive à l'utilisation de l'accès conditionnel pour des raisons de droit d'auteur, ont fait l'objet d'une discussion approfondie. Une telle extension permettrait aux détenteurs de droits d'auteur - parallèlement aux prestataires de services protégés et indépendamment d'eux - d'intenter une action en dommages et intérêts et de demander une compensation aux fabricants et aux vendeurs de dispositifs illicites.

Finalement, il a été décidé de ne pas inclure la protection des droits d'auteur dans la directive. L'une des principales raisons en a été que, vu l'état du droit communautaire

¹⁶ Cette approche est communément utilisée dans la législation relative au marché intérieur. Elle figure dans la communication de la Commission sur l'importance des sanctions pour la mise en œuvre de la législation communautaire – COM(95)162 et, pour la première fois, approuvée par la Cour de justice dans son jugement de l'affaire 68/88, Commission contre Grèce [1989] REC-2965.

¹⁷ Le considérant 23 précise que les États membres ne sont pas obligés d'imposer des sanctions pénales.

¹⁸ Le considérant 22 permet, par exemple, un “test de connaissance” en ce qui concerne les activités illicites. Le considérant 23 permet, par exemple, la saisie des dispositifs illicites.

à cette époque, la production et la vente des dispositifs illicites n'auraient pu être considérées comme une violation des droits d'auteur¹⁹. Une autre raison devait être trouvée dans la négociation en cours d'un projet de directive relative aux droits d'auteur dans la société de l'information, qui contenait des dispositions sur des mesures de protection techniques et d'anticonournement, et qui était considérée comme un complément à la directive "Accès conditionnel"²⁰. La Commission a accepté de commander une étude visant à examiner les implications juridiques et économiques de l'utilisation d'un accès conditionnel pour des raisons autres que la protection de la rémunération²¹. L'étude, qui a été terminée en avril 2000, se concentrait sur les "intérêts qui ne sont pas régis par la disposition relative à toute forme de paiement financier direct par le destinataire en contrepartie de la fourniture d'un service par le prestataire de service/de contenu".

L'étude a identifié un grand nombre de ce type d'intérêts qui vont du respect des obligations contractuelles et statutaires, des stratégies commerciales et publicitaires, des aspects de sécurité à la rémunération indirecte. Dans tous les cas, l'étude a estimé que la décision d'utiliser un accès conditionnel était basée sur des considérations juridiques et économiques valables. Certains de ces intérêts concernaient les organismes de diffusion et d'autres, les prestataires de services de la société de l'information. Elle montre que l'accès conditionnel est fréquemment utilisé pour plus d'une raison en même temps. Apparemment, les exigences de l'industrie du contenu (droits d'auteur) et l'utilisation de techniques de transmission très étendue (satellites) sont les principales forces motrices à l'origine de l'utilisation de l'accès conditionnel pour des raisons autres que la rémunération.

L'étude prévoit que l'utilisation de l'accès conditionnel pour des raisons autres que la rémunération va augmenter, mais qu'il est encore trop tôt pour prévoir sérieusement et de manière fiable comment évoluera le marché et quelles seront les conséquences de l'utilisation accrue de l'accès conditionnel. L'étude indique que le risque de piratage sera similaire dans les cas de rémunération et de non-rémunération.

2.3.2. *Objectifs commerciaux/objectifs privés*

La liste des activités illicites dressée dans la directive se base essentiellement sur celle des activités illégales figurant dans la recommandation R(91)14 du Conseil de l'Europe²². Cette directive et la recommandation qui l'a précédée (théorie) estiment que le moyen le plus efficace d'empêcher le piratage consiste à se concentrer sur les activités commerciales permettant des accès illégaux.

Au moment de la discussion de la directive, un petit nombre d'États membres avaient décidé que certains actes privés seraient passibles de sanctions (détention à des fins privées d'un dispositif illicite et/ou réception privée non autorisée elle-même). Durant la discussion de la directive, les États membres et les institutions communautaires avaient des avis divergents quant à la nécessité et à la possibilité

¹⁹ Le considérant 21 de la directive précise que la directive "Accès conditionnel" ne porte pas atteinte à l'application des règles communautaires en matière de propriété intellectuelle.

²⁰ Voir COM(97)628final du 10.12.1997, p. 33.

²¹ Cette étude a été confiée à l'"Institute for Information Law (IVIR)" de l'Université d'Amsterdam. Le rapport final (avril 2000) est disponible sur le site <http://www.ivir.nl/publications/other/ca-report.htm> ou sur le site http://europa.eu.int/comm/internal_market/fr/media/condac/backgrnd/index.htm

²² Pour de plus amples informations, voir chapitre 6 du présent rapport.

d'étendre l'harmonisation des activités illégales à des activités autres que commerciales. Finalement, il a été convenu que la directive ne couvrirait que les activités commerciales mais que les États membres auraient la possibilité d'interdire, dans leur législation nationale²³, la détention à des fins privées de dispositifs illicites.

Des discussions du même type ont eu lieu lors de l'adoption de la directive sur les droits d'auteur dans la société de l'information et ont abouti à une solution plus ou moins comparable²⁴.

3. MISE EN ŒUVRE DE LA DIRECTIVE

3.1. Communication des mesures de mise en œuvre

La directive octroie aux États membres une période d'un an et demi pour mettre en œuvre ses dispositions. Le 28 mai 2000 (délai fixé pour la transposition), seuls quelques États membres avaient communiqué les mesures de transposition à la Commission.

Conformément à la procédure fixée à l'article 226 du traité (ancien article 169) qui concerne la non-communication des mesures nationales de mise en œuvre, des lettres de mise en demeure ont été envoyées aux États membres défaillants. Suite à la réception de ces lettres, une grande majorité d'États membres ont communiqué leurs mesures de mise en œuvre.

À la date de cette communication, la Commission a été obligée de saisir la Cour de justice à l'encontre de plusieurs États membres (Grèce et Espagne) pour non-communication²⁵.

Plusieurs communications ne contiennent pas toutes les informations nécessaires qui permettraient à la Commission d'évaluer le niveau de mise en œuvre, au plan national, des mesures et leur compatibilité avec la loi communautaire. Afin de clarifier cette situation, des discussions bilatérales ont actuellement lieu entre la Commission et les États membres concernés. Le cas échéant, la Commission entamera des procédures d'infraction en vertu de l'article 226 contre les États membres qui, selon elle, n'appliquent pas la directive avec la spécificité, la précision et la clarté requises²⁶.

3.2. État actuel de la mise en œuvre par les États membres

Il s'est écoulé beaucoup de temps entre l'entrée en vigueur de la directive et l'adoption des législations nationales relatives à son application. La plupart des législations sont entrées en vigueur à partir du second semestre de l'année 2000.

²³ Voir considérant n° 21 de la directive.

²⁴ Pour de plus amples informations, voir directive 2001/29/CE, articles 6.1, 6.2 et 6.3 et considérant n° 49; JO L167 du 22.06.2001, p. 10.

²⁵ Espagne : affaire C-58/02 ; Grèce : affaire C- 219/02 ; Communiqué de presse de la Commission IP/02/455 du 22.03.2002;

http://europa.eu.int/comm/internal_market/fr/media/infr/02-455.htm

²⁶ Affaire C-197/96, paragraphes 14 et 15

Année	État membre
<1998	France – Pays-Bas
1999	
2000	Autriche – Irlande – Italie – Suède – Royaume-Uni
2001	Danemark – Finlande – Portugal
2002	Allemagne – Luxembourg – Grèce
Plus tard	Belgique — Espagne

tableau 2: année d'entrée en vigueur

Un tableau, constamment mis à jour, de la mise en œuvre de la directive par les États membres de l'UE et de l'EEE ainsi que par les pays candidats - y compris de nombreuses références aux législations nationales et des traductions non officielles en anglais - est disponible sur le site EUROPA²⁷.

Comme on pouvait s'y attendre, les États membres ont transposé la directive dans leur législation nationale de différentes manières. Certains ont choisi d'utiliser, d'une part, la législation sur les médias pour couvrir les services classiques de radio et de télévision et, d'autre part, la législation sur la cybercriminalité (ou législation associée) pour les services de la société de l'information et les services à part entière d'accès conditionnel. D'autres États membres ont préféré une seule disposition (ou série de dispositions) couvrant tous les services soit dans le code pénal, soit dans une législation spéciale.

Dans l'ensemble, les mesures de mise en œuvre au niveau national communiquées à la Commission satisfont aux exigences de la directive. Dans un grand nombre d'États membres, tous les services protégés sont correctement couverts même si l'on ne sait pas clairement si les services d'accès conditionnel à part entière sont effectivement protégés dans quelques États membres. Certains points mineurs nécessitant des précisions font encore l'objet de discussions entre la Commission et l'État membre concerné.

La situation est sensiblement la même en ce qui concerne la série d'activités illicites qu'il convient d'interdire conformément à l'article 4 de la directive. Dans un petit nombre de cas, une activité illégale particulière n'est pas formellement interdite car on part du principe qu'elle est couverte par un terme plus générique ou sanctionnée en vertu d'une disposition générale figurant dans le code pénal national. Afin de garantir une certaine obligation juridique pour les citoyens et l'industrie, la Commission discute de ces cas avec l'État membre concerné.

Tandis que la directive n'oblige pas les États membres à imposer des sanctions pénales²⁸, tous les États membres à l'exception de deux (Italie, Portugal) punissent d'emprisonnement et/ou d'amende ce qu'ils considèrent être les principales activités illégales (fabrication et vente). Manifestement, il existe certaines divergences d'appréciation, au niveau national, de la nature illégale des activités interdites et des moyens de dissuasion indispensables.

²⁷

http://europa.eu.int/comm/internal_market/fr/media/condac/natimp/index.htm

²⁸

Considérant n° 23, deuxième phrase, de la directive

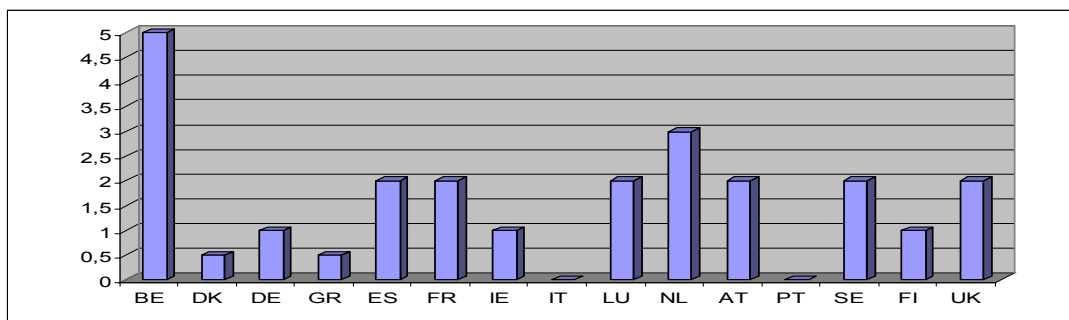


diagramme 1 : peine maximum d'emprisonnement en années pour les principales activités illégales

Quelques États membres ont introduit un système de sanctions modulées. L'inclusion des interdictions et des sanctions dans le droit pénal fait que l'on dispose également de la liste classique des délits secondaires (complicité, instigation, aide et incitation) ainsi que des procédures pénales (recherche et saisie, confiscation).

Dans quelques États membres (Autriche, Allemagne, Italie) où des dispositions juridiques existant déjà ont pu être utilisées pour poursuivre en justice certaines formes de piratage, l'introduction de sanctions spécifiques mais moins sévères, concernant les activités illégales définies par la directive s'est soldée par une réduction *de facto* de la protection juridique dans ces États membres²⁹.

Dans la plupart des États membres, des voies de droit appropriées existent pour les prestataires de services lésés. Pour les quelques cas dont on ne sait pas réellement si toutes les voies de droit requises par la directive ont été proposées, la Commission demande des précisions à l'État membre concerné.

La Commission conclut que la transposition de la directive dans la législation nationale n'apparaît pas à ce stade complètement terminée dans tous les États membres. Deux États membres n'ont pas encore achevé ce processus de transposition tandis que pour plusieurs autres pays, quelques incertitudes subsistent quant à l'exhaustivité et à la compatibilité de cette transposition. La Commission va poursuivre son examen des dispositions en vigueur ainsi que ses efforts pour que la directive soit totalement mise en œuvre.

3.3. Dispositions nationales allant au delà des exigences de la directive

La directive ne propose qu'un niveau minimum de protection juridique contre le piratage et laisse aux États membres une souplesse et une latitude certaines pour adapter leur réglementation nationale antipiratage à leurs besoins et politiques propres. Plusieurs États membres ont fait usage de cette prérogative et élargi la définition des services protégés ainsi que des activités illégales, des sanctions et des voies de droit.

Un nombre important d'États membres n'exigent pas explicitement l'utilisation de l'accès conditionnel et ne se limitent pas seulement à la rémunération du prestataire de service, mais garantissent la protection de tous les services contre les accès non autorisés ou les accès sans permission.

²⁹ Lex specialis derogat generali

De même, une minorité d'États membres interdit l'utilisation et/ou la détention de dispositifs illégaux à des fins privées.

Certains États membres ont prévu des sanctions (publication des jugements, confiscation des profits) et des voies de droit spécifiques (compensation de pertes de profits, transferts des profits réalisés).

Dans quelques États membres, une autorité de surveillance nationale (il s'agit parfois de l'autorité des télécommunications ou bien d'un service spécial) a été chargée de contrôler et de surveiller le marché et l'application (partielle) de la loi.

3.4. Élargissement

Les pays candidats doivent mettre en œuvre la directive dans le cadre de l'*acquis communautaire*. La mise en œuvre en temps voulu, accompagnée d'une application effective, est de la plus haute importance pour combattre le piratage au sein de l'Union ainsi que dans les pays en voie d'adhésion. Parallèlement au renforcement de la protection dans l'UE, les actes de piratage liés à la télévision à péage et aux services internet ont progressivement tendance à se déplacer vers l'Europe centrale.

L'élargissement est l'une des principales priorités de la Commission en 2002³⁰ et 2003³¹. La Commission contrôle activement le processus de mise en œuvre et aide, autant que faire se peut, les pays candidats à élaborer puis à mettre en œuvre la législation nationale permettant d'appliquer la directive.

Bien que des efforts importants soient encore nécessaires, les progrès réalisés jusqu'à présent sont encourageants. Quatre pays ont déjà mis en place une grande partie de la législation requise. Plusieurs autres pays candidats préparent actuellement leur projet de législation de mise en œuvre et envisagent une adoption finale pour la fin de l'année 2003. Les pays restants ont confirmé qu'ils avaient l'intention d'adopter les mesures nécessaires pour l'adhésion et donc au plus tard, en 2004.

Comme cela a déjà été souligné dans le précédent chapitre du présent rapport, l'application de la législation en vigueur est une tâche primordiale pour les autorités nationales. Les autorités chargées de l'application de la législation dans les pays candidats devront être formées afin d'être prêtes à appliquer la législation une fois que celle-ci sera entrée en vigueur.

La mise en œuvre de la directive progresse de manière encourageante dans les pays candidats même si des efforts importants doivent encore être faits.

La Commission continuera à travailler avec l'ensemble des pays candidats afin qu'ils acquièrent un niveau adéquat de capacité administrative et judiciaire au moment de leur adhésion³². Des séminaires spéciaux de formation³³ pour les autorités policières et judiciaires peuvent être envisagés³³ avec le concours d'acteurs du secteur industriel spécialisé.

³⁰ COM(2001)620final du 05.12.2001, p. 14

³¹ Voir communiqué de presse IP/02/338 (Stratégie politique annuelle pour 2003).

³² COM(2002)256final du 05.06.2002

³³ Voir également chapitre 4.3 sur l'application.

4. ÉVOLUTIONS DU MARCHÉ ET APPLICATION DE LA DIRECTIVE

4.1. **Consultation des acteurs du marché**

Lors de la préparation du présent rapport, la Commission a consulté les principaux partenaires industriels touchés par le piratage des services protégés d'accès conditionnel et leur a demandé leur avis sur les parades juridiques correspondantes. Conformément à l'engagement pris dans son Livre blanc sur la gouvernance européenne³⁴ et à ses récentes propositions sur la façon de mieux légiférer³⁵, la Commission a entrepris cette consultation afin d'encourager un dialogue ouvert sur les problèmes de piratage affectant le marché et d'aider à collecter et à analyser les informations nouvelles et existantes dans le domaine, techniquement et juridiquement avancé, couvert par la directive. La Commission n'a pas commencé à en évaluer l'impact global³⁶ étant donné que la transposition de la directive dans la législation nationale était encore en cours pendant la période de référence.

Les résultats de la consultation ont grandement contribué à la préparation du présent rapport et à son éventuel suivi³⁷. Manifestement, les acteurs du marché répugnent à discuter en détail du piratage et de la manière dont il affecte leurs activités. Trop d'ouverture peut s'avérer contreproductive étant donné l'impact potentiel sur la confiance des clients quant à la qualité de la protection offerte, la position concurrentielle sur le marché et la valeur actionnariale. Des associations industrielles telles que AEPOC³⁸, STOP³⁹ ou l'ICRT⁴⁰ ont joué un rôle très important en exprimant les préoccupations et en illustrant les problèmes des membres qu'elles représentent. Bien que compréhensible, cette attitude protectrice complique les efforts faits pour avoir un tableau clair de l'étendue et de l'impact du problème ainsi que pour trouver des solutions effectives et efficaces.

En échange, et conformément aux efforts faits pour communiquer de manière plus active avec l'opinion publique sur les questions européennes, la Commission a totalement remanié ses pages sur le site EUROPA consacrées à la directive et à sa mise en œuvre⁴¹.

³⁴ COM(2001)428final du 25.07.2001; http://europa.eu.int/comm/governance/index_fr.htm

³⁵ COM(2002)275final et COM(2002)277final du 05.06.2002

³⁶ COM(2002)276final du 05.06.2002

³⁷ La Commission a reçu des contributions écrites des organismes suivants: AEPOC, EBU, AER, ACT, MPA, ACTI, ACCeS, DVD, STOP Sweden, STOP Denmark, STOP Norway, ICRT et du Groupe Kirch. De plus, des réunions bilatérales plus informelles ont eu lieu avec plusieurs acteurs du marché.

³⁸ L'AEPOC, l'Association européenne pour la protection des œuvres et services cryptés, représente Betaresearch, BskyB, Canal+, Canal+Polska, Canal+ technologies, Conax, Eutelsat, IrdetoAccess, Motorola, NDS, NTV-Plus, Pace, Philips Digital Networks, Première, Rai, SCM Microsystems, Société Européenne des Satellites, Sogecable, Stream, Tele+, Thompson, TPS, UPC et Viaccess-France Telecom; voir <http://www.aepoc.org/>.

³⁹ STOP (organisations scandinaves de TV contre le piratage) existe en Finlande, en Suède, en Norvège et au Danemark (<http://www.stop.dk>).

⁴⁰ L'ICRT (the International Communications Round Table) représente American Express, AOL Time Warner, Springer, Bertelsmann, British Telecom, Coface, EDS, IBM, Kirch, Philips, KPN, Lagardère, Microsoft, NCR, News Int, NewsCorp, Reed-Elsevier, Reuters, Siemens, Sony, Walt Disney, UPC, von Holtzbrinck, Vivendi, VNU, Yahoo (www.icrt.org)

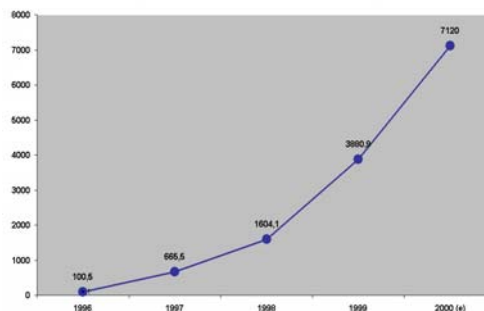
⁴¹ http://europa.eu.int/comm/internal_market/fr/media/condac/index.htm

4.2. Combattre le pir@tage – une cible mouvante

Le piratage audiovisuel et, en particulier, le piratage des services à péage se développe parallèlement aux services dont il tente de profiter. Au départ, il était possible de pirater des canaux de TV payante analogique cryptés en modifiant des décodeurs. Ce type de piratage nécessitait une connaissance spécialisée de la technologie et de l'électronique de la TV analogique, ainsi que des compétences spéciales de fabrication.

Services visés par les pirates

La numérisation a amplifié la multiplication des canaux de distribution et l'offre de contenu d'où, *inter alia*, un développement rapide du marché de la télévision numérique à péage. Depuis 1996, les revenus d'abonnement croissent de façon exponentielle. De récentes études de la Commission montrent que l'importance des abonnements progresse régulièrement. Les revenus d'abonnement à la télévision numérique sont passés de moins de 25% des recettes de l'industrie en 1995 à 35% environ en 2000.



source: IDATE et 7^{ème} rapport de mise en œuvre Telecom

graphique 2: revenus des abonnements à la TV numérique depuis 1996 (en millions d'euros)

Du fait du passage à la numérisation des réseaux câblés analogiques et de la télévision terrestre, les services de TV numérique à péage sont progressivement fournis via ces nouveaux canaux de distribution (voir détails dans le tableau 3). Des statistiques récentes confirment plus ou moins cette tendance et montrent que vers 2008, la TV numérique sera présente dans 73% des foyers européens (122 millions de ménages)⁴².

La prolifération de la TV numérique se traduira par une importante utilisation de décodeurs numériques, soit sous la forme de matériels (boîtiers et téléviseurs intelligents) ou de logiciels (logiciels spécialisés sur un PC avec une carte DVB⁴³).

L'aspect négatif de cette convergence technique est que l'actuel piratage de la TV numérique par satellite touchera de nouveaux domaines, tels que la télévision numérique terrestre et la télévision numérique par câble, et deviendra un phénomène de plus en plus répandu.

⁴² Strategy Analytics, 28 mai 2002; <http://www.strategyanalytics.com/press/prsk012.htm>

⁴³ Une carte DVB est un matériel informatique conçu pour recevoir, décoder et diffuser la télévision numérique selon les normes DVB européennes installé sur un ordinateur personnel standard.

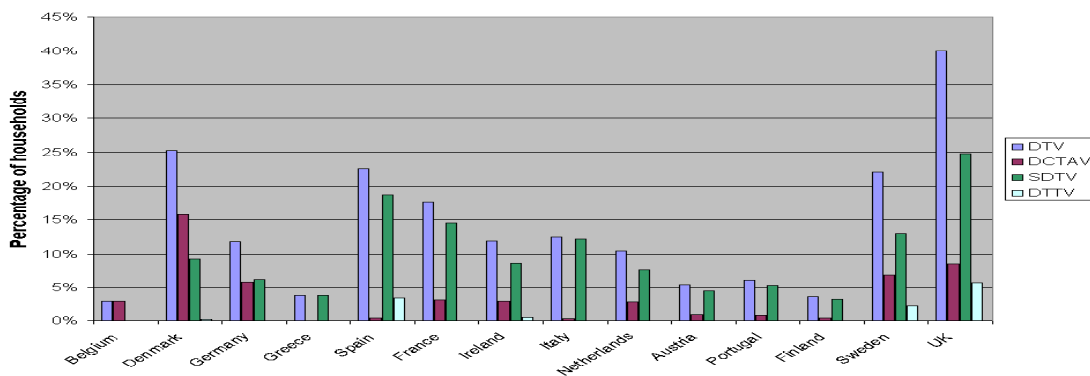
Ménages possédant une TV numérique	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Satellite											
Ménages (M) possédant une TV numérique par satellite	0.0	0.4	1.9	4.1	8.3	14.3	19.2	24.0	28.2	32.3	35.9
Câble											
Ménages (M) possédant une TV numérique par câble	0.0	0.0	0.1	0.8	1.7	3.2	6.1	10.7	16.3	22.5	28.8
Terrestre											
Ménages (M) possédant une TV numérique terrestre	0.0	0.0	0.0	0.0	0.5	1.3	2.1	3.5	5.1	7.1	8.8
TOTAL DES MÉNAGES (M) POSSÉDANT UNE TV NUMÉRIQUE	0.0	0.4	2.0	5.0	10.5	18.7	27.4	37.8	48.7	60.1	70.8

Source: Strategy Analytics, février 2001 et 7^{ème} rapport de mise en œuvre Telecom

Tableau 3: Ménages possédant une TV numérique dans l'UE (plus Norvège et Suisse), évolution et prévisions

Les marchés nationaux de la télévision numérique se trouvent à des stades très différents de développement dans les États membres. Les écarts, en termes de pénétration, entre les différents modes de transmission de la TV numérique influenceront le niveau du piratage dans chaque État membre (voir détails dans le graphique 3).

Contrairement à la TV à péage, les services de radio à péage en Europe ne sont pas, jusqu'à présent, très répandus. En Europe, la radio est, en majorité, captée en clair⁴⁴. Quelques stations de radio à péage fonctionnent aux USA, mais uniquement par le biais d'un capteur breveté et d'une technique d'accès conditionnel. Ces stations font la promotion de leurs services à péage en soulignant la haute qualité du son, la couverture de l'ensemble du pays et la grande variété des programmes musicaux, sportifs et d'informations sans message publicitaire. En Europe, il n'existe pas encore d'expérience similaire, mais on s'attend à un développement des radios à péage par le biais de services radiophoniques numériques, par exemple en combinaison avec d'autres technologies telles que la téléphonie mobile.



Source : préparé par les services de la Commission européenne sur la base de données tirées de "Strategy Analytics

DTV: TV numérique
DCAV: DTV par câble
SDTV: DTV par satellite
DTTV: TV numérique terrestre

Graphique 3: Ménages UE possédant une TV numérique en 2001, par État membre et mode de transmission (pourcentage de ménages)

⁴⁴

Il arrive que des chaînes de radio thématiques ne soient disponibles que pour les souscripteurs de "paquets" très avantageux; voir, par exemple, http://www4.telepiu.it/v4_intrattenimento/multimusica/multimusica.asp

Du fait du ralentissement de l'économie virtuelle (internet) et de la faiblesse du marché publicitaire, les prestataires de services de la société de l'information lancent des services de grande qualité contre rémunération afin de générer d'autres sources de revenu et de créer des relations durables avec leurs clients. Ces services d'abonnement par internet sont essentiellement protégés par l'identificateur de l'utilisateur/le mot de passe et vont des jeux en ligne, des recherches de documents avancées, d'offres de journaux et de revues spécialisées en ligne aux téléchargements de musiques et aux films à la demande. Les services de mise à jour en ligne, dont disposent les propriétaires de logiciels originaux, sont une catégorie de services payants qui marche bien; à cet égard, le numéro de série du CD original fonctionne comme une autorisation d'accès. Les acteurs du marché et les législateurs observent actuellement, avec grand intérêt et espoir, ces premières tentatives (probablement encore prématurées) de générer des revenus à partir d'offres de contenus en ligne.

Méthodes et instruments de piratage

La plupart des actes de piratage actuels de la TV numérique à péage touchent la carte à puce ou le logiciel de décodage. Une large gamme de sites web et de forums de discussion fournissent une information de base approfondie sur les différents systèmes d'accès conditionnel, des instructions sur la façon de (re)programmer les cartes à puce ainsi que des références permettant de "trouver" les clés essentielles. La technologie de la carte à puce est couramment utilisée pour des applications commerciales. Le matériel et le logiciel permettant de programmer ces cartes sont largement disponibles car les cartes à puce et leurs programmeurs sont également utilisés à des fins légitimes. Il est évident que la convivialité des instruments nécessaires et la disponibilité de connaissances et d'informations sur internet ont considérablement facilité les piratages de systèmes numériques.

Les cartes à puce pirates proviennent souvent des cartes originales fournies par les opérateurs de TV à péage. Les cartes désactivées ou les cartes ne donnant accès qu'à l'offre de services de base sont modifiées (on les appelle les MOSC⁴⁵) et sont transformées en cartes donnant totalement accès à l'ensemble des services. Les cartes à puce pirates numériques (Digital Pirate Smart Cards ou DPSC) sont des "clones" de cartes originales à fonctions identiques ou des cartes à puce nouvellement programmées.

Les pirates professionnels sont bien équipés et produisent un grand nombre de MOSC et de DPSC. La production et la distribution quasi-industrielles de ces cartes pirates exigent des méthodes de travail hautement "professionnelles" qui se rapprochent souvent du crime organisé.

La production "locale", à une échelle beaucoup plus petite, de cartes pirates utilisant des cartes à puce vierges accessibles au public a un caractère moins industriel qui n'en est pas moins préjudiciable. Ce type de pirates utilise du matériel "faites-le-vous-même" et des informations principalement accessibles via internet. Les profits proviennent de la vente de cartes vierges et de programmeurs ou d'installations complètes de réception par satellite, y compris une carte d'accès pirate⁴⁶ pour un prix

⁴⁵

Modified Original Smart Card ou Carte à puce originale modifiée

⁴⁶

Les coûts marginaux nécessaires à la production de ce type de carte sont insignifiants (moins de 1%) en comparaison des coûts réels de l'abonnement.

avantageux. Le crime organisé utilise également ces pirates pour distribuer de fausses cartes produites par des pirates professionnels. La nature commerciale de cette forme de piratage est souvent difficile à établir car les auteurs prévoyants réduisent au minimum leur risque "pénal".

Certains particuliers participent également à cette forme de piratage que l'on pourrait qualifier "d'artisanat familial". En tant que "pirates occasionnels", ils utilisent le même matériel et les mêmes informations et proposent des cartes "faites maison" pour rendre un petit service à des amis, à des voisins ou à des collègues de travail, souvent contre de l'argent ou en échange d'autres biens tels que des copies pirates de logiciels, de CD musicaux ou de DVD.

De plus en plus, des personnes techniquement très "calées" produisent des cartes pirates pour leur usage propre. La seule chose qu'elles aient à faire est d'acquérir le savoir-faire nécessaire à partir de sites pirates et de procéder à un investissement modeste et unique dans le matériel de base.

Deux formes de piratage, relativement nouvelles et extrêmement dangereuses, sont en train de se développer rapidement. La première consiste à utiliser un PC ordinaire équipé de cartes TV DVB et de décodeurs de logiciels. Ces décodeurs puissants, qui imitent le matériel d'accès conditionnel et la carte à puce, sont distribués via internet. La seconde forme résulte de la possibilité de modifier des modules d'accès conditionnel à interface commune (CAM) disponibles dans le commerce en appliquant des correctifs de logiciels spécialisés, de sorte qu'il n'est plus nécessaire d'avoir une carte à puce en cours de validité (FreeCams). Ces deux formes se basent sur une distribution très conviviale via internet qui font d'elles un logiciel meurtrier potentiel.

À l'exception des plus professionnels, tous les pirates ont besoin que des clés, des instruments de contournement des mesures de protection, des instructions, etc. soient disponibles sur des sites pirates privés sur le web. Ces sites sont le lien essentiel dans la chaîne d'activités de piratage car ils fournissent le matériel nécessaire. Mais ils sont également le talon d'Achille d'une grande partie des activités de piratage. Nombre de ces sites pirates se présentent eux-mêmes comme des initiatives privées sans aucun concours économique de partenaires commerciaux. Même si cela peut être vrai pour certains d'entre eux, d'autres utilisent des bannières publicitaires ou recommandent des marques particulières de produits, ce qui s'apparente à une certaine forme de relation commerciale. Les sites web ont besoin d'ordinateurs centraux et de connexions internet qui ne sont jamais gratuits.

Dommages causés par le piratage

Le piratage audiovisuel n'est pas un crime "sans victime". La plupart des télédiffuseurs à péage ont des marges financières étroites. L'écart entre la réussite commerciale et la faillite est habituellement très faible dans ce type d'industries émergentes. Souvent, le sort de ces diffuseurs dépend d'un accroissement progressif d'une audience payante et d'un revenu moyen par abonné (ARPU⁴⁷). Le nombre de téléspectateurs pirates regardant un programme sans payer peut faire la différence.

⁴⁷

Average Revenue per User ou Revenu moyen par abonné

Le piratage ne prive pas seulement les opérateurs de leurs revenus, il accroît également les coûts de fonctionnement ainsi que la nécessité d'investissements supplémentaires. Selon des sources industrielles, le remplacement d'une carte à puce dans le cadre d'un échange à grande échelle coûte environ 11€⁴⁸. Un important opérateur de TV à péage a déclaré qu'il avait dépensé plus de 35 millions d'euros pour mettre au point son intergiciel de décodage et son système d'accès conditionnel qui sont très largement utilisés⁴⁹.

Le piratage peut également avoir des conséquences négatives pour les recettes du Trésor public national. Les pirates ne paient pas de taxe sur leurs services; les fournisseurs légaux paient moins de TVA et de taxes sur les sociétés en raison d'une baisse de leur chiffre d'affaires et de leurs profits.

Les consommateurs respectueux des lois peuvent facilement être trompés sur l'origine des décodeurs et des cartes à puce. Ils sont les premiers à subir les conséquences d'un comportement frauduleux des pirates lorsque l'opérateur désactive leurs cartes à puce pirates ou prend d'autres mesures de rétorsion.

Indirectement, le piratage perturbe également d'autres marchés de l'audiovisuel. Il touche non seulement le commerce de détail des décodeurs et des abonnements mais, il a également un effet potentiellement préjudiciable sur le secteur du cinéma et de la location de vidéocassettes ou de DVD étant donné que l'existence du matériel haut de gamme est accessible via un accès illégal aux services électroniques à péage.

Les informations fournies par l'AEPOC⁵⁰, l'Association européenne pour la protection d'œuvres et de services cryptés, ont montré que les pertes de revenu, en Europe, dues au piratage en 1996 étaient supérieures à 200 millions d'euros. L'AEPOC estime qu'en raison de la croissance du chiffre d'affaires légal annuel des opérateurs de TV à péage, le chiffre d'affaires illégal lié au piratage est de l'ordre de 1 milliard d'euros chaque année. Récemment, ITV Digital a calculé que ses pertes de revenu dues au piratage de cartes à puce dépassaient 100 millions de livres⁵¹.

Outre les dommages sur le plan économique, les actes de piratage eux-mêmes engendrent également des dommages pour la société. Les vols en tous genres sont, par définition, inadmissibles dans toute société civilisée car ils portent atteinte à notre système de valeurs. Les équivalents cybernétiques de ces délits et les dommages causés à l'intérêt public devraient être jugés de la même façon.

Parades

Les opérateurs de TV à péage luttent depuis longtemps contre le piratage. Dans les premiers temps de la TV à péage, les opérateurs ont évité d'entamer des actions judiciaires afin que l'opinion publique n'aie pas conscience de la vulnérabilité de leurs services. La première réponse au piratage a donc été l'adoption de parades techniques. Aujourd'hui, les opérateurs exploitent toutes les possibilités de parades de leurs systèmes actuels, notamment les mises à jour de clés et le blocage de cartes à puce pirates connues.

⁴⁸ Marchés des nouveaux médias – 31.05.2002, p. 6

⁴⁹ Marchés des nouveaux médias – 15.03.2002, p. 5

⁵⁰ <http://www.aepoc.org/>

⁵¹ Marchés des nouveaux médias – 15.03.2002, p. 5

De manière permanente et systématique, les opérateurs contrôlent également le marché du piratage et analysent les méthodes et équipements pirates nouveaux afin de se maintenir au courant du piratage et de riposter par des contre-attaques. Ils limitent la vulnérabilité de leurs systèmes en perfectionnant le cryptage et en développant les systèmes de clés utilisés pour identifier les utilisateurs (individuels). Récemment, plusieurs grands opérateurs ont remplacé toutes les cartes à puce légales par d'autres plus sûres. Ce remplacement de millions de cartes constitue, pour ces opérateurs, un défi logistique majeur dont le coût montre leur détermination à combattre le piratage.

Toutefois, il existe des limites pratiques à ces efforts étant donné les coûts que cela représente, les désagréments pour les utilisateurs légitimes et les possibilités techniques du système concerné. À ce stade, la mise en œuvre effective d'une protection juridique constitue la prochaine ligne de défense.

4.3. Assurer le respect

La plupart des États membres n'ont aligné leurs législations nationales sur la directive que récemment. Par conséquent, il est encore trop tôt pour dresser un tableau complet des effets pratiques de cette nouvelle législation sur le piratage et le combat qui est mené contre lui. Les autorités réglementaires nationales ainsi que les acteurs du secteur concerné doivent se familiariser avec le nouveau cadre juridique et apprendre à exploiter de manière optimale ses possibilités.

Lors des consultations de la Commission, plusieurs acteurs du marché ont déclaré être préoccupés par la mise en œuvre inégale de la directive et la réticence des autorités nationales à enquêter sur les personnes suspectes et à les poursuivre. Ils ont attiré l'attention sur le fait que le piratage audiovisuel est un délit complexe tant sur le plan technique que juridique, et ont insisté sur la nécessité et leur volonté de coopérer, d'aider et, le cas échéant, de sensibiliser les autorités nationales en conjuguant leurs efforts. Plusieurs exemples de partenariats efficaces contre les pirates ont montré qu'une telle approche peut réussir et devrait encourager les autorités et les prestataires de services qui ne participent pas à cette action à s'engager dans cette voie bénéfique pour tous. Une coopération pratique devrait voir le jour grâce à des séminaires de formation, à la création de réseaux dynamiques de personnes et d'autorités concernées par la lutte contre ce type de piratage, et aux échanges des meilleures pratiques et d'informations dans toute l'Union élargie⁵².

La plupart des personnes interrogées soulignent les changements radicaux du piratage grâce à l'internet et déplorent que l'actuel cadre juridique n'ait pas été conçu en tenant compte de ce type de menaces. La nature commerciale des sites pirates est souvent difficile à établir. Les informations-clés nécessaires sont aisément accessibles sur internet et permettent à des individus de rendre des services "pirates" à des amis, la plupart du temps sans objectif commercial. Ils critiquent le fait que des cartes vierges et des programmeurs ne soient qualifiés de dispositifs illicites que dans des circonstances très particulières. Les auteurs peu scrupuleux sont conscients

⁵²

Un exemple type de ce genre d'effort conjoint est le projet e-S.P.A.C.E. Dublin 2001 mis en place grâce au programme Falcone de l'Union européenne, dans le cadre duquel le travail d'équipe du Irish Garda National Bureau d'investigation criminelle avec Microsoft a conduit à la production d'un CD de formation sur la piraterie et la contrefaçon de logiciels

de ces faiblesses de la loi et adaptent leurs méthodes de travail afin de rester le plus longtemps possible en dehors de l'illégalité.

Parfois, certaines autorités semblent s'abstenir d'intervenir sur la base du Code pénal et pressent les prestataires de services à se défendre eux-mêmes, en première instance, en entamant des procédures civiles devant les tribunaux. Bien qu'acceptable dans certains cas, ce type de politique n'encourage pas les prestataires de services à informer le public des cas de piratage et peut leur refuser la protection offerte par le droit pénal. Ils s'exposent, en outre, aux risques de demandes reconventionnelles en dommages ou pour publicité négative. Les réticences des deux côtés se traduisent par un manque de données fiables sur l'ampleur et le type du piratage, ce qui complique davantage l'élaboration de politiques et l'application du droit.

Tous les acteurs du marché demandent que la définition des activités illégales couvre, au moins, la détention privée et l'utilisation personnelle de dispositifs illégaux. Dans les pays nordiques, cette approche semble avoir permis de réprimer avec succès le piratage.

Même si elles reconnaissent le niveau différent de la protection, quelques personnes interrogées ont souligné la similitude entre les mesures d'application, les procédures à suivre et les autorités nationales responsables de l'application de la législation relative au piratage des accès conditionnels d'une part, et celles chargées de combattre la contrefaçon et le piratage des droits d'auteur, d'autre part.

La Commission encourage les États membres et les pays candidats à mettre en œuvre des mesures d'exécution et à protéger, comme il convient, les prestataires de services à péage contre les pirates qui s'enrichissent à leurs dépens.

La Commission continuera à consulter les États membres et les pays candidats sur les difficultés de mise en œuvre qui subsistent afin d'identifier et de combler les lacunes de la législation.

L'industrie et les autorités chargées de l'application de la législation devraient continuer à lutter ensemble pour réprimer le piratage.

La Commission continuera à soutenir, autant que possible, ces développements dans le cadre des programmes de financement comme le programme cadre AGIS sur la coopération policière et judiciaire en matière pénale⁵³ ainsi que des ressources disponibles pour aider les pays candidats à accroître leur capacité administrative et judiciaire.

4.4. Pratiques commerciales exposées au piratage

Régulièrement, l'attention de la Commission est attirée sur le fait que des citoyens ne peuvent accéder à des programmes de TV par satellite protégés émis par un État membre autre que celui dans lequel ils résident, et qui sont aisément accessibles, à peu de frais, par l'intermédiaire d'antennes paraboliques⁵⁴, et ce, en dépit du fait que

⁵³ http://europa.eu.int/comm/justice_home/funding_agis_en.htm

⁵⁴ En ce qui concerne le "droit d'utiliser une antenne parabolique", la Commission a adopté une communication sur l'application des principes généraux de libre circulation des biens et des services –

ces citoyens sont prêts à payer pour y accéder. Les prestataires de services prétendent souvent qu'ils ne détiennent pas les droits pour le pays de résidence de ces citoyens et qu'ils sont obligés d'utiliser les techniques d'accès conditionnel afin de limiter l'accès et de protéger les droits d'auteur. Les citoyens n'arrivent pas à comprendre qu'au sein du marché intérieur, ils ne peuvent légitimement accéder aux services de TV à péage protégés, même s'ils sont prêts à payer un abonnement et les frais d'exécution.

Manifestement, ces pratiques incitent beaucoup les téléspectateurs concernés (expatriés, professionnels et étudiants intéressés par d'autres cultures ou pays) à "supprimer" cet obstacle en ayant recours à des équipements illégaux. Les revenus générés par la vente de ces équipements illégaux vont aux pirates et non aux diffuseurs et aux détenteurs de droits. Les parades antipiratage normales qui désactivent les cartes pirates ne réduisent pas le piratage à l'extérieur car les non-résidents utilisant des cartes pirates ne peuvent se procurer, par des voies légitimes, des cartes à puce valables et doivent donc se tourner vers les pirates s'ils souhaitent continuer à regarder la télévision nationale. Ce type d'activité stimule la demande de cartes illégales, encourage le piratage, entraîne des citoyens respectueux de la loi à enfreindre cette dernière et nie l'existence du marché intérieur.

L'autorisation de droits sur une base strictement nationale a également fait l'objet de travaux dans le cadre de la directive 93/83/CE relative à la coordination de certaines règles du droit d'auteur et des droits voisins du droit d'auteur applicables à la radiodiffusion par satellite et à la retransmission par câble⁵⁵. Les services de TV à péage constituent le cas le plus simple de transmissions transfrontières de TV par satellite. Les titulaires de droits négocient avec les diffuseurs les termes et les conditions de diffusion de leurs œuvres. La rémunération est souvent proportionnelle à l'audience attendue. En utilisant les techniques d'accès conditionnel, il est tout-à-fait possible de déterminer exactement l'audience à l'extérieur du territoire d'origine (le prestataire de service sait à qui – nombre et lieu de résidence - il a vendu ses cartes) et de collecter les redevances auprès des téléspectateurs (ils ont acheté une carte). L'accès conditionnel permet aux diffuseurs de servir les clients non résidents et de verser aux titulaires de droits la rémunération correspondante.

La prévention et des mesures astucieuses pour neutraliser les possibilités de piratage entraînent non seulement une réduction *de facto* du piratage mais augmentent également la crédibilité des appels à une protection juridique plus importante contre les actes de piratage qui persistent.

La Commission a déjà publiquement annoncé qu'elle procédait à l'examen des différents aspects de ce problème et tentait de concilier, de manière transparente et équilibrée, les différents intérêts, notamment le droit à une rémunération équitable pour les détenteurs de droits, les pratiques commerciales des télédiffuseurs par satellite et les libertés fondamentales contenues dans le traité⁵⁶.

articles 28 et 49 CE; (COM(2001)351final du 27.06.2001);
http://europa.eu.int/comm/internal_market/fr/media/satdish/index.htm

⁵⁵ JO L248 du 06.10.1993, p.15; voir le site

http://europa.eu.int/comm/internal_market/fr/media/cabsat/index.htm

⁵⁶ Le récent rapport de la Commission sur l'application de la directive 93/83/CE relative à la radiodiffusion par satellite et à la retransmission par câble conclut que la liberté de réception et de transmission de programmes TV d'autres États membres est réduite si les problèmes qu'implique le transfert du droit d'auteur et des droits voisins ne sont pas résolus: COM(2002)430final du 26.07.2002

La Commission appelle les prestataires de services électroniques à péage à rechercher activement les moyens de prévenir et de réduire le piratage en mettant au point, par exemple, avec les détenteurs de droits des solutions contractuelles en vue de fournir aux abonnés non résidents un accès aux services électroniques à péage protégés à des conditions raisonnables, non discriminatoires et transparentes si ces services sont, par nature, disponibles dans tout le marché intérieur.

5. AUTRES DEVELOPPEMENTS JURIDIQUES CONCERNANT LA FOURNITURE DE SERVICES D'ACCES CONDITIONNEL

5.1. L'adoption de la directive 2001/29/CE sur le droit d'auteur dans la société de l'information

Après trois ans de discussion approfondie, l'adoption de la directive 2001/29/CE⁵⁷ en mai 2001 constitue une étape importante qui facilite les échanges transfrontières de biens et de services protégés par des droits d'auteur. Cette directive, qui est actuellement mise en œuvre par les États membres, complète la protection juridique offerte par la directive "accès" et couvre, en particulier, la protection juridique des dispositifs anticopie et des systèmes de gestion de droits. Elle satisfait certaines des préoccupations exprimées par les détenteurs de droits à propos du manque de protection accordé par la directive "accès".

Indépendamment du champ actuel d'application de la directive 2001/29/CE, il se pourrait que certains développements techniques et modèles commerciaux récents soient à prendre en compte à long terme.

Au départ, les techniques d'accès conditionnel ne protégeaient que le signal transmis par le prestataire de service. La nouvelle génération de réseaux numériques et de magnétoscopes personnels maintient l'accès conditionnel au fur et à mesure que se développe la consommation d'appareils numériques⁵⁸. L'accès conditionnel tend à devenir une composante d'un système de protection élargi visant à fournir une protection complète du contenu tout au long du processus, depuis la diffusion initiale jusqu'au moment où l'utilisateur final verra et entendra le programme⁵⁹. La gestion de l'accès conditionnel et des droits numériques peut faire appel au même "dispositif" de cryptage dans l'équipement multimédia domestique⁶⁰.

En même temps, l'industrie recherche de nouvelles possibilités d'exploiter - de façon souvent inattendue et originale - les technologies disponibles afin d'offrir un nouveau contenu motivant et d'optimiser la création et les revenus⁶¹. Ces nouveaux modèles

⁵⁷ JO L167 du 22.06.2001, p. 10

⁵⁸ La nouvelle génération de magnétoscopes numériques n'utilise plus de bandes vidéo mais enregistre directement sur le disque dur; les programmes enregistrés ne peuvent être vus qu'à l'aide d'une carte à puce en cours de validité.

⁵⁹ Le projet de radiodiffusion télévisuelle numérique (DVB) s'intéresse actuellement à la mise au point d'un nouveau système de protection des contenus et de gestion des copies (CPCM) (www.dvb.org).

⁶⁰ Pour de plus amples informations de base et d'exemples, voir le document de travail de la Commission sur les droits numériques; SEC(2002)197 du 14.02.2002.

⁶¹ Les nouveaux services musicaux en ligne tels que Pressplay (entreprise commune Vivendi/Sony) sont protégés par un accès conditionnel mais impliquent également la gestion des droits des titres téléchargés ou transmis en continu. On constate des développements similaires dans le secteur de la vidéo à la demande dans lequel des films de qualité sont disponibles par abonnement et peuvent être téléchargés

économiques ont fréquemment un caractère expérimental, tout au moins au début, et ignorent le cadre juridique applicable.

Cette convergence technologique ne se traduit pas nécessairement et automatiquement par une convergence juridique, comme par exemple le regroupement de plusieurs instruments de protection juridique en un seul⁶². Il convient toutefois de contrôler étroitement les développements du marché afin de garantir que la loi offre une protection harmonieuse et complémentaire. À l'inverse, il faut éviter la surprotection pour ne pas freiner l'innovation, le développement économique ou limiter abusivement les droits des utilisateurs qui comprennent des droits fondamentaux tels que la liberté d'expression ou le respect de la vie privée et la protection des données.

Compte tenu de ces évolutions juridiques, commerciales et techniques, la Commission estime inopportun de proposer une extension du champ de la protection juridique offerte par la directive à l'utilisation de l'accès conditionnel pour des raisons de droit d'auteur.

5.2. L'adoption d'un nouveau cadre réglementaire pour les services de communications électroniques

En mars 2002, le Conseil et le Parlement européen ont approuvé une série de directives et une décision fixant le nouveau cadre réglementaire pour les réseaux et les services de communications électroniques⁶³. Cette série a été complétée par une directive sur la vie privée dans les communications électroniques adoptée le 12 juillet 2002⁶⁴.

Cet ensemble représente une révision majeure de la législation communautaire sur les télécommunications qui libéralise davantage les marchés concernés tout en adaptant les règles en vue d'une convergence technologique. Il couvre les réseaux et services de communications électroniques, notamment les réseaux et services de diffusion et les ressources associées. Le régime spécifique des systèmes d'accès conditionnel fixé dans la directive 95/47/CE relative à l'utilisation de normes pour la transmission de signaux de télévision⁶⁵ est également modifié.

D'après le nouveau cadre pour les communications électroniques, les "systèmes d'accès conditionnel" font partie de ce que l'on appelle les "ressources associées"⁶⁶. L'obligation d'offrir l'accès aux services d'accès conditionnel de façon juste, raisonnable et non discriminatoire et les conditions d'interopérabilité pour l'accès conditionnel, qui avaient d'abord été fixées dans la directive 95/47/CE⁶⁷, ont

via internet; la visualisation du film est contrôlée. Après la première visualisation, l'abonnement peut être renouvelé en ligne et en temps réel.

⁶² Voir également note de bas de page n° 10.

⁶³ IP/02/259 du 14.02.2002. Directive 2002/19/CE (Directive Accès) ; Directive 2002/20/CE (Directive Autorisation) ; Directive 2002/21/CE (Directive Cadre) ; Directive 2002/22/CE (Directive Service Universel) ; Décision 676/2002/CE (Décision spectre radio) : JO L 108, 24.04.2002.

⁶⁴ Directive 2002/58/CE; JO L201 du 31.07.2002

⁶⁵ JO L281 du 23.11.1995, p. 51 (abrogé à partir du 25.07.2003);

http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

⁶⁶ Directive 2002/21/CE; JO L108 du 24.04.2002, p. 33; article 2(e) et (f)

⁶⁷ La directive 95/47/CE prévoyait, *entre autres*, l'utilisation de l'algorithme commun d'embrouillage géré par l'ETSI (cet algorithme spécifie comment le dispositif de déchiffrement du décodeur déchiffre la

été reprises dans le nouveau cadre bien que sujettes à modifications⁶⁸. En particulier, l'accès conditionnel aux services de radio numérique est maintenant couvert et les procédures d'analyse de marchés en vue de la révision des obligations liées à l'accès conditionnel aux services de télédiffusion numérique ont été introduites qui, en particulier, autorisent les Etats membres, sous certaines conditions, de modifier ou de supprimer les obligations d'accès imposées aux opérateurs sans part de marché significative⁶⁹. Les systèmes et services d'accès conditionnel ne sont pas couverts par la directive "Autorisation"⁷⁰.

Bien que n'offrant pas une protection juridique contre le piratage des services d'accès conditionnel, ce cadre pro-compétitif gère la fourniture de réseaux et de services de communications électroniques en général et les systèmes d'accès conditionnel en particulier; en tant que tel, il est très important pour l'évolution du marché dans les années à venir.

La Commission contrôlera de près les évolutions futures des marchés de l'accès conditionnel dans le nouveau cadre réglementaire relatif aux communications électroniques, quand il sera déterminé si des mesures antipiratage complémentaires peuvent s'avérer nécessaires.

5.3. La mise en œuvre de la directive 2000/31/CE sur le commerce électronique

Bien que la législation communautaire comporte une définition des services de la société de l'information depuis l'adoption de la directive 98/48/CE⁷¹, les États membres ont été obligés d'introduire un ensemble important de règles et de réglementations concernant les services de la société de l'information, du fait de la seule adoption de la directive sur le commerce électronique⁷².

La mise en œuvre de la directive sur le commerce électronique accroîtra la sécurité juridique pour les industriels et les consommateurs et favorisera le développement rapide de tous les types de nouveaux services interactifs sur internet, y compris ceux protégés par un accès conditionnel et fournis contre rémunération.

Dans le cadre de la mise en œuvre de la directive sur l'accès conditionnel, la plupart des États membres ont déjà introduit la notion de "services de la société de l'information" dans leur système juridique. Afin de maintenir une certaine sécurité juridique, les États membres ne devraient pas inclure de définitions différentes ou contradictoires dans leur législation nationale.

diffusion protégée), la possibilité de capter des transmissions en clair ainsi que le connecteur d'interface commune DVB (il s'agit d'une interface standardisée entre un module d'accès conditionnel enfichable et interchangeable et le décodeur, ce qui permet d'utiliser dans le même décodeur plusieurs techniques d'accès conditionnel différentes).

⁶⁸ Directive 2002/22/CE; JO L108 du 24.04.2002, p. 51; article 24 et annexe VI

⁶⁹ Directive 2002/19/CE; JO L108 du 24.04.2002, p. 7; articles 2(a), 6 et annexe I

⁷⁰ Directive 2002/20/CE; JO L108 du 24.04.2002, p. 21; considérant n° 6.

⁷¹ Directive 98/48/CE, JO L217 du Parlement européen et du Conseil du 20 juillet 1998 portant modification de la Directive 98/34/CEE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques ; JO L 217 du 05.08.1998.

⁷² Directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur (directive sur le commerce électronique); JO L178 du 17.07.2000, p. 1-16

La directive sur le commerce électronique prévoit, *entre autres*, une série de règles communes limitant la responsabilité de certains prestataires de services intermédiaires, comme par exemple les prestataires de services d'hébergement⁷³. Ces règles couvrent la responsabilité pour tous types d'activités illégales initiées par des parties tierces en ligne et incluent la diffusion d'informations liées au piratage, ou même de dispositifs illicites par l'intermédiaire de sites web, de nouveaux groupes et de forums de discussion⁷⁴.

La Commission s'assurera que toute initiative à venir portant sur l'accès conditionnel sera cohérente avec la directive sur le commerce électronique.

5.4. La proposition d'une décision-cadre du Conseil relative aux attaques visant les systèmes d'information

Récemment, la Commission a adopté une proposition de décision du Conseil relative aux attaques visant les systèmes d'information⁷⁵. Ce projet cherche à rapprocher les lois criminelles à travers l'Union européenne afin d'assurer qu'en Europe, les autorités judiciaires sur base de ces lois puissent prendre des actions contre les plus nouvelles formes d'activité criminelle contre les systèmes d'information et a pour objectif de compléter ce qui a déjà été réalisé dans le domaine du droit communautaire en vue de protéger les systèmes d'information, et est sans préjudice du droit communautaire⁷⁶.

La proposition de décision-cadre couvre, *entre autres*, l'accès non autorisé à un ordinateur ou à des réseaux d'ordinateurs, notamment l'accès aux services protégés par un accès conditionnel sans paiement. La proposition reconnaît que les dispositifs d'accès conditionnel tels que les décodeurs numériques et les magnétoscopes personnels sont, *de facto*, des "ordinateurs" et que les services protégés d'accès conditionnel sont fournis par le biais d'un "système d'information"

Si l'approche proposée par la Commission était retenue par le Conseil, les États membres seraient tenus d'ériger en infraction "l'accès illégal aux services d'information" si elle est commise contre un système d'information faisant l'objet de mesures de protection particulières (par exemple, un service de TV à péage par satellite utilisant un accès conditionnel), ou avec l'intention de porter préjudice (par exemple au fournisseur d'une technologie ou de services d'accès conditionnel) ou avec l'intention d'obtenir un avantage économique (par exemple, en réalisant des bénéfices par la vente de dispositifs illicites)⁷⁷. La proposition ne fait aucune distinction entre le fait de commettre cette infraction à des fins privées ou commerciales et n'exige pas que le service soit fourni contre rémunération. Elle

⁷³ L'article 14, paragraphe 1, de la directive sur le commerce électronique décharge les prestataires de services intermédiaires stockant des informations accessibles au public fournies par leurs clients (les services d'hébergement) de toute responsabilité pour l'information stockée si certaines conditions n'ont pas été remplies.

⁷⁴ Les procédures de "retrait" du matériel, une fois qu'il a été notifié au prestataire de services concerné qu'il pouvait avoir un caractère illégal, sont particulièrement importantes. La directive sur le commerce électronique ne régleme pas ces procédures de "notification et de retrait", mais fournit un cadre pour développer des mécanismes d'autoréglementation.

⁷⁵ COM(2002)173final du 19.04.2002.

⁷⁶ Voir en particulier article 47 du traité sur l'Union européenne, le considérant n° 18 du projet de décision-cadre et COM(2002)173 paragraphe 1.6.

⁷⁷ Projet de décision-cadre, article 3

n'exige pas non plus que dans tous les cas, il ait été nécessaire que les systèmes d'accès conditionnel soient contournés pour qu'il y ait infraction.

La décision-cadre proposée complète la protection juridique offerte par la directive relative à l'accès conditionnel et fournit un niveau supplémentaire de protection contre le piratage des services à péage protégés d'accès conditionnel.

6. COMBATTRE LE PIRATAGE – UN EFFORT PAN-EUROPEEN

6.1. Recommandation n° R(91)14 sur la protection juridique des services de télévision cryptés

Dès septembre 1991, le Conseil de l'Europe a adopté une recommandation sur la protection juridique des services de télévision cryptés⁷⁸. Cette recommandation a inspiré les législateurs d'un grand nombre de pays européens⁷⁹ et a servi de tremplin à la directive de l'UE et à son pendant, la convention européenne sur l'accès conditionnel.

La recommandation représente la première génération de la protection juridique. Elle protège exclusivement les services de télévision utilisant des techniques de cryptage et ne fait pas de distinction entre les services payants et gratuits ou entre les différentes raisons d'utiliser le cryptage.

Point intéressant, la recommandation note qu'il incombe aux fournisseurs de services de télévision cryptés d'utiliser les meilleures techniques de cryptage disponibles.

Selon la recommandation, toutes les activités commerciales et privées liées à la fabrication, à l'importation, à la distribution et à la promotion commerciale de matériels de décodage permettant l'accès par ceux qui sont extérieurs au public déterminé par le prestataire de service, sont considérées comme illicites. La détention à des fins commerciales est également considérée comme illicite. En ce qui concerne la détention de matériels de décodage à des fins privées, les États membres sont libres de décider que cette détention doit être considérée comme une activité illicite.

La recommandation insiste sur les sanctions pénales et administratives appropriées ainsi que sur la confiscation de décodeurs saisis et des profits financiers résultant d'activités illicites.

Avec le temps, on a constaté que le Conseil de l'Europe, qui a été le premier à tenter de compléter la protection technique par une protection juridique, a contribué à l'établissement d'un consensus parmi les pays européens sur la façon de combattre efficacement le piratage.

⁷⁸ <http://cm.coe.int/ta/rec/1991/91r14.htm>

⁷⁹ Sur la base de cette recommandation, la législation protégeant les services de TV cryptés a été adoptée, au début des années 90, par plusieurs pays comme le Danemark, la Finlande, la France, l'Irlande, les Pays-Bas et le Royaume-Uni.

6.2. Convention européenne STE n° 178 sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel

Pour répondre au piratage croissant, les États membres du Conseil de l'Europe ont, parallèlement à l'adoption de la directive, entamé des négociations sur un instrument similaire et contraignant. La Commission a négocié cette convention au nom de la Communauté et de ses États membres sur la base d'un mandat donné par le Conseil le 12 juin 1999.

Lors de la négociation de la convention, la Commission a veillé tout particulièrement à ce que la directive et la convention concordent autant que possible. La convention couvre *grosso modo* les mêmes questions que la directive et envisage explicitement que la Communauté européenne puisse y adhérer.

Depuis l'ouverture aux signatures le 24 janvier 2001, la convention a été signée par trois États membres de l'UE et par trois pays candidats⁸⁰. Jusqu'à présent, Chypre et la Roumanie ont formellement ratifié la convention. D'autres pays candidats ont déclaré adhérer à la convention. La convention exige l'accord de trois États pour entrer en vigueur.

Pour fournir un cadre juridique pan-européen cohérent et un niveau égal de protection contre le piratage dans l'ensemble de l'Europe, il est important que la convention n° 178 du Conseil de l'Europe entre en vigueur dès que possible. La Commission travaillera en vue de la ratification de cette convention.

6.3. La situation juridique dans les autres pays européens

Conformément aux dispositions de l'accord sur l'Espace Économique Européen, le comité mixte de l'EEE a décidé, le 28 février 2001⁸¹, d'inclure la directive dans les annexes X et XI de l'accord. Cette décision est entrée en vigueur le 1^{er} octobre 2001; l'application pratique est gérée par les règles et procédures de l'EEE. Parmi les trois pays non-UE participants, seul le Liechtenstein n'a pas encore adopté la législation de mise en œuvre. La Norvège a signé la convention n° 178 du Conseil de l'Europe et a modifié son code pénal en conséquence⁸². L'Islande a modifié sa législation sur les médias⁸³.

La Suisse a signé la convention n° 178 du Conseil de l'Europe et prépare actuellement la ratification formelle et la mise en œuvre au niveau national.

San Marin, Monaco et Andorre n'ont pas de législation spécifique relative au domaine couvert par la directive. Le manque de législation adéquate peut être à l'origine de lacunes dans la structure pan-européenne de la protection juridique contre le piratage et risque de réduire l'efficacité de la protection juridique en créant des sphères de sécurité pour les pirates.

⁸⁰ Le texte intégral de la convention, le rapport explicatif et la situation actuelle en ce qui concerne les signatures et la ratification se trouvent sur le site

<http://conventions.coe.int/Treaty/FR/WhatYouWant.asp?NT=178&CM=8&DF=>

⁸¹ Décision n° 17/2001 du 28.02.2001; JO L117 du 26.04.2001, p. 21

⁸² Code pénal norvégien, article 262 en vigueur depuis le 01.08.2001

⁸³ Broadcasting Act n° 53 (loi sur la radiodiffusion et la télévision) du 17.05.2000

La Commission encourage les pays, qui ne seront pas membres de l'Union européenne élargie de conjuguer leurs efforts à ceux de la Communauté afin d'atteindre un niveau égal de protection contre la piraterie dans l'ensemble de l'Europe.

6.4. Convention européenne STE n° 185 sur la cybercriminalité

Afin de mener une lutte commune contre la cybercriminalité, le Conseil de l'Europe a préparé une convention sur la cybercriminalité qui est ouverte à la signature depuis le 23 novembre 2001⁸⁴. À la date de l'établissement du présent rapport, cette convention a été signée par treize États membres de l'UE, plusieurs pays candidats ainsi que par certains autres États.

La convention oblige les États adhérents à ériger en infractions pénales conformément à leur droit interne, *entre autres*, l'accès illégal aux services d'information et, plus important encore, l'usage abusif de dispositifs. Les dispositions relatives à l'utilisation abusive de dispositifs, énoncées à l'article 6 de cette convention, interdisent la série classique d'activités (par exemple, fabrication, vente, diffusion, détention, etc.) associées à ces dispositifs ainsi que l'utilisation abusive de mots de passe et de codes d'accès informatiques, et présentent un intérêt particulier en raison de leur portée et de leur nature générale ainsi que des possibilités qu'elles offrent pour stopper le piratage lié à internet.

La participation de pays non européens permet d'espérer l'adoption de mesures globales, ce qui est particulièrement important pour combattre les activités illicites liées à internet. La coopération transatlantique concernant la mise en œuvre et le contrôle des dispositions de la convention relative à la lutte contre le piratage de l'accès conditionnel, devrait être approfondie et si possible étendue à d'autres domaines.

Même si la Communauté ne peut adhérer à cette convention, les solutions qu'elle propose pour les questions liées à l'accès conditionnel devraient être prises en compte et, éventuellement, utilisées comme modèle pour d'autres mesures de lutte contre le piratage au sein de l'UE.

7. CONCLUSIONS ET PROCHAINES ETAPES

7.1. Les services électroniques payants sont importants pour une économie basée sur la connaissance arrivant à maturité

Actuellement, les services électroniques payants existent surtout dans le secteur de la TV numérique à péage. Durant la présente décennie, on s'attend à une prolifération massive de toutes sortes de nouveaux services électroniques payants fournis par tous les réseaux possibles de distribution. Les premiers exemples de services de la société de l'information par abonnement offrant des contenus de grande qualité via internet ont récemment fait leur apparition. La numérisation des réseaux câblés ainsi que l'introduction de la télévision numérique terrestre, des communications mobiles de

⁸⁴ Le texte intégral de la convention, le rapport explicatif et la situation actuelle en ce qui concerne les signatures et la ratification se trouvent sur le site <http://conventions.coe.int/Treaty/FR/WhatYouWant.asp?NT=185&CM=8&DF=>

3^{ème} génération et de services de transport avancés se traduira, dans un futur qui n'est pas si lointain, par un déploiement à grande échelle de dispositifs intelligents capables de développer des services à péage. De nouveaux équipements électroniques grand public, comme par exemple le "ciné maison" (integrated home entertainment centres) et les magnétoscopes personnels, seront conçus pour améliorer l'écoute et la visualisation même si des techniques d'accès conditionnel sont utilisées et qu'un accès n'est possible que contre paiement.

Les économies basées sur la connaissance du 21^{ème} siècle devraient progressivement se fonder sur une généralisation des services électroniques payants. En conséquence, l'intérêt de ces services pour l'économie et la société s'accroîtra dans le temps. La fraude et le piratage liés aux services à péage auront tendance à se développer au même rythme que les services à péage eux-mêmes, à moins qu'une protection juridique adéquate et une application efficace soient garanties. Le piratage de services électroniques payants a les mêmes conséquences néfastes dans la société de la connaissance que la criminalité en col blanc et la contrefaçon de biens au 20^e siècle. L'Union doit tenir compte de cette évolution si elle souhaite réaliser l'objectif ambitieux de devenir l'économie la plus dynamique et la plus compétitive d'ici 2010⁸⁵.

Il est donc important de donner à l'industrie et aux citoyens un signal clair montrant que la Communauté et ses États membres ne peuvent accepter que le développement de l'économie et de la société dans l'Union soit sévèrement entravé par des actes de piratage, et qu'ils doivent engager des actions d'utilité publique. Un signal précoce et fort peut prévenir un niveau de piratage toléré et socialement accepté, comme c'est le cas actuellement dans le domaine de la musique numérique.

La Commission considère les services électroniques payants comme la composante essentielle de l'économie basée sur la connaissance qui se développe. La protection juridique contre le piratage des services électroniques payants est le facteur essentiel d'évolution de ces services et une condition sine qua non de la croissance et de la prospérité futures pour les citoyens de l'Union.

7.2. Renforcement de la protection juridique actuelle – actions à entreprendre

Dans sa forme actuelle, la directive offre déjà un niveau important de protection juridique contre le piratage des services électroniques payants protégés par un accès conditionnel. Comme le montre le présent rapport, il est encore possible d'améliorer la protection juridique actuelle sans modifier la directive.

La mise en œuvre n'est pas encore totalement achevée dans l'Union élargie et l'application au niveau national doit être consolidée. L'industrie et les autorités réglementaires nationales devraient continuer à développer leurs partenariats publics/privés en conjuguant leurs efforts pour réprimer le piratage avec, si possible, l'aide financière de l'Union.

Combattre avec succès le piratage implique également des mesures de prévention actives afin de réduire les zones floues dans lesquelles le piratage peut prospérer. Les

⁸⁵

Conseil européen de Lisbonne, 23-24 mars 2000; conclusions de la Présidence, section 5

télespectateurs payants non résidents devraient pouvoir capter des programmes de TV à péage par satellite protégés.

Il sera possible de combattre efficacement le piratage si les pirates ne peuvent trouver de sphères de sécurité en Europe. Une entrée en vigueur rapide de la convention n° 178 du Conseil de l'Europe contribuera, de manière décisive, à atteindre cet objectif.

En résumé, l'efficacité de la directive peut être renforcée par les actions suivantes:

- La Commission est déterminée à poursuivre ses efforts pour que la directive soit totalement mise en œuvre. Elle travaillera avec les États membres et les pays candidats pour garantir la totale application de la directive et pour résoudre toutes les questions juridiques qui se posent encore. Le cas échéant, la Commission entamera des procédures d'infraction.
- La Commission consultera les États membres à propos des difficultés pratiques qu'ils rencontrent dans l'application des dispositions nationales de mise en œuvre de la directive.
- La Commission encouragera l'industrie et les autorités nationales à conjuguer leurs efforts en vue de combattre le piratage de manière aussi efficace et rationnelle que possible.
- La Commission continuera à coopérer avec d'autres pays européens et les organisations internationales concernées afin d'appliquer, de manière cohérente, les règles européennes contre le piratage des services électroniques payants.
- La Commission recommande aux détenteurs de droits et aux prestataires de services de rechercher activement des solutions contractuelles afin que les abonnés non-résidents puissent accéder aux services électroniques payants protégés à des conditions raisonnables, non discriminatoires et transparentes dans tout le marché intérieur. La Commission contribuera à ce processus dans le cadre de la révision de la directive 93/83/CE.

7.3. Renforcer la protection juridique – et ensuite?

Le piratage des services électroniques payants protégés par un accès conditionnel fait partie de la cybercriminalité qui s'est profondément modifiée ces dernières années. Même si l'actuelle protection juridique est relativement efficace contre les formes classiques de piratage, il convient de renforcer la protection afin de pouvoir faire face aux nouvelles catégories d'infraction, à l'incidence de l'internet, et de répondre à certaines questions de mise en œuvre qui restent à résoudre.

Étant donné les possibilités de protection que l'on peut attendre des actions supplémentaires prises en vertu de la directive actuelle, la Commission estime qu'il serait prématuré de proposer des modifications de la directive sur la base du présent rapport, mais qu'une révision de la directive peut être envisagée dans le cadre d'une série cohérente de mesures juridiques contre toutes les formes possibles de piratage.

Toutefois, les consultations et évaluations faites dans le contexte du présent rapport ont permis à la Commission de déterminer déjà les questions suivantes qui méritent

une réflexion approfondie en étroite coopération avec les États membres et l'industrie:

- Les formes industrielles du piratage sont clairement d'ordre commercial et sont donc déjà couvertes par la directive "Accès". Ce type de piratage est très semblable à la contrefaçon de produits ou au piratage des droits d'auteur. Un cadre de mise en œuvre, équilibré et cohérent, applicable à tout type de piratage et de contrefaçon, et approuvé au niveau communautaire, devrait renforcer l'efficacité de la protection juridique des services électroniques payants.
- On a estimé que les pirates occasionnels et les individus se livrant au piratage à des fins exclusivement personnelles pourraient être poursuivis, notamment pour des activités illégales qui ne sont pas exercées à des fins commerciales et/ou de détention privée de dispositifs illicites. Toutefois, une extension de la directive "Accès" dans ce sens exigerait une modification fondamentale de la politique communautaire et pourrait avoir un impact sur la législation connexe.
- La directive actuelle n'est pas très efficace contre les formes de piratage qui sont apparues par le biais d'internet. L'un des moyens de combattre ces formes de piratage est d'interdire la diffusion directe et indirecte de clés et de dispositifs illicites via l'internet. De plus, les prestataires de services concernés peuvent être tenus de retirer ce type de dispositifs (notification et retrait). Ces mesures visent la principale source de nombreux actes de piratage et peuvent éviter d'autres mesures plus radicales contre des personnes privées. L'article 6 de la convention du Conseil de l'Europe sur la cyber-criminalité présente déjà un modèle pour ce type de mesure. Dans ce contexte, la Commission n'envisage aucune mesure restreignant la diffusion d'informations techniques détaillées sur le système d'accès conditionnel car cela limiterait abusivement la liberté d'expression et freinerait l'innovation.

La Commission continuera à étudier l'application de la directive "Accès Conditionnel" et ses rapports avec d'autres dispositions de la loi communautaire. Elle verra s'il est nécessaire ou non de modifier la directive et invite les États membres, les pays candidats et d'autres parties intéressées à participer à ce travail.