



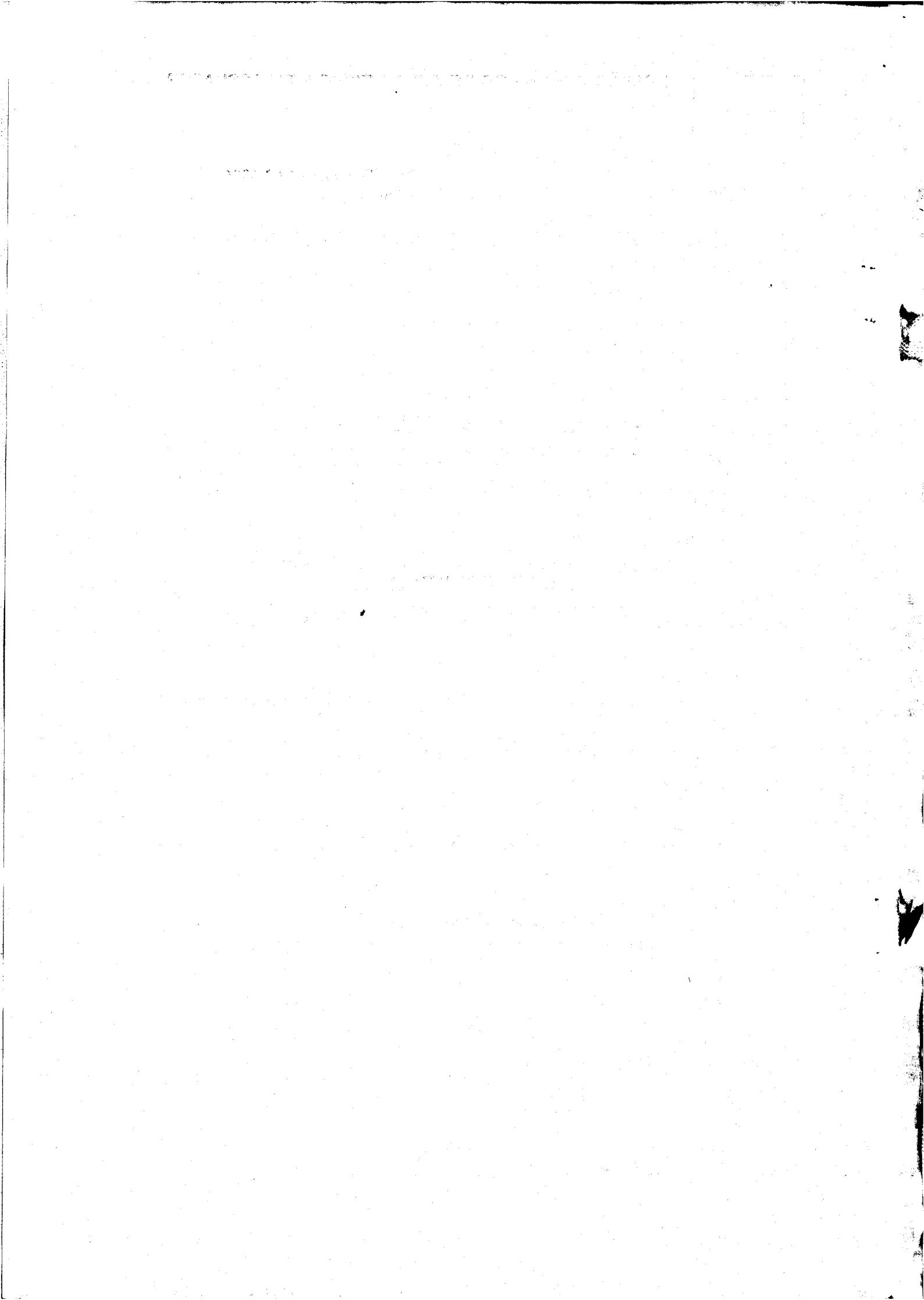
KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 06.03.1996
KOM(96) 76 endelig udg.

**RETLIG BESKYTTELSE AF
KRYPTEREDE TJENESTER
I DET INDRE MARKED**

**HØRING OM BEHOVET
FOR EN EF-FORANSTALTNING**

Grønbog udarbejdet af Kommissionen



GRØNBOG OM RETLIG BESKYTTELSE AF KRYPTEREDE TJENESTER I DET INDRE MARKED

Resumé

Indledning

KAPITEL 1: DET EUROPÆISKE MARKED FOR KRYPTEREDE TJENESTER

1. Et marked i hastig udvikling
2. Et europæisk marked
3. Et marked, der er udsat for piratvirksomhed
4. Et marked med forskellig lovgivning

KAPITEL 2: DE INTERNATIONALE REGLER

1. Arbejdet i Europarådet
2. Arbejdet i WIPO

KAPITEL 3: LOVGIVNINGEN I MEDLEMSSTATERNE

1. Generelt
2. Den lovgivningsmæssige situation i medlemsstaterne (oversigt)

KAPITEL 4: HINDRINGERNE FOR DET INDRE MARKEDS FUNKTION

1. Hindringer for den frie bevægelighed for dekoderudstyr (traktatens artikel 30 ff.)
2. Hindringer for den frie bevægelighed for dekoderudstyr (traktatens artikel 59 ff.)
3. Hindringer for den frie udveksling af krypterede tjenester
4. Konkurrenceforvridning

KAPITEL 5: BEHOVET FOR EN EF-FORANSTALTNING OG MULIGE INITIATIVER

1. Formålet med initiativet
2. Overensstemmelse med Fællesskabets øvrige politik
3. Valg af instrument og retsgrundlag
4. Anvendelsesområde
5. Generel arkitektur

LISTE OVER SPØRGSMÅL

Resumé

Formål

De seneste års stigende tilrådighedsstillelse af frekvenser og anvendelsen af nye teknologier har gjort det muligt at udvikle nye radio- og tv-spredningstjenester med krypterede signaler, hvorved modtagelsen begrænses til de personer, der har betalt licens. For at modtage programmet, skal modtageren anskaffe dekoderudstyr, der kan genskabe originalbilledet.

Disse tjenester udgør et marked i hastig udvikling, bl.a. takket være den digitale teknik, der vil gøre det muligt at øge kommunikationskapaciteten. På grund af disse tjenesters særlige karakteristika vil den tværnationale - ofte europæiske - dimension være helt afgørende. Denne udvikling er imidlertid truet af piratvirksomhed. Faktisk eksisterer der parallelt med de officielle fabrikanter af dekoderudstyr en blomstrende uautoriseret industri. Uden operatørernes godkendelse fremstiller og markedsfører denne industri udstyr, der muliggør modtagelse af de omhandlede tjenester uden licensbetaling. Denne ulovlige modtagelse medfører betydelige tab for tjenesteudbydere og er indirekte et angreb på programindustrien og de officielle fabrikanters udnyttelsesmuligheder.

Kommissionen understregede derfor allerede i det strategiske program for det indre marked af 22. december 1993 (KOM(93) 632), at det var vigtigt at sikre en retlig beskyttelse af krypterede tjenester mod ulovlig modtagelse.

Et sådant krav er endnu vigtigere i lyset af informationssamfundet. De nye krypterede tjenester vil blive mangedoblet i fremtiden, og uanset tjenesternes indhold er det nødvendigt at beskytte dem mod ulovlig modtagelse.

Derfor annoncerede Kommissionen i meddelelsen "Europa på vej mod informations-samfundet - en handlingsplan" (KOM(94) 347), at den ville udarbejde en "Grønbog om retlig beskyttelse af krypterede tjenester i det indre marked" for at undersøge de problemer, der på den ene side følger af, at der i nogle medlemsstater ikke findes lovgivning om retlig beskyttelse af krypterede tjenester, og på den anden side af de forskelle, der findes i de øvrige medlemsstaters lovgivning.

Den lovgivningsmæssige situation

Det fremgår af den sammenlignende analyse af medlemsstaternes lovgivning, at de forsøger at løse problemet med ulovlig modtagelse af krypterede tjenester på vidt forskellige måder.

Nogle medlemsstater vedtog allerede i slutningen af 80'erne en særlovgivning om beskyttelse af krypterede tjenester mod ulovlig modtagelse, mens andre medlemsstater (A, P, E, GR, DK, D, LUX) endnu ikke har en sådan lovgivning.

Den generelle lovgivning, der i nogle tilfælde anvendes i de sidstnævnte medlemsstater (f.eks. lovgivning om illoyal konkurrence, telekommunikation, ophavsret) giver ofte ikke en effektiv beskyttelse mod ulovlig modtagelse af krypterede tjenester. Det har betydet, at der i nogle medlemsstater er opstået en blomstrende piratindustri, der fremstiller, markedsfører, installerer og vedligeholder piratudstyr. Endvidere er der dukket en fagpresse op med målrettede reklamer og oprettelse af særlige forhandlernet af piratudstyr. Denne situation smitter af på de andre medlemsstater, hvor dette udstyr, på trods af restriktive foranstaltninger, findes på markedet.

I de lande, hvor der findes en særlovgivning, er der betydelige forskelle i de valgte løsninger, bl.a. hvad angår anvendelsesområde, forbudte aktiviteter (salgsfremme, privatpersoners besiddelse) og de tilsvarende sanktioner.

Behovet for en EF-foranstaltning

I lyset af denne situation synes der at være et behov for en EF-foranstaltning. Hvis der ikke findes samme retsbeskyttelse i alle medlemsstater, vil det indre marked ikke kunne fungere. Situationen medfører en række hindringer for den frie udveksling af krypterede tjenester, og dekoderudstyret betyder konkurrenceforvridning mellem operatørerne i de forskellige medlemsstater. De nuværende forskellige lovgivningsmæssige løsninger med de ekstraomkostninger og den manglende retssikkerhed, der følger deraf, er ifølge branchefolkene én af de væsentligste hindringer for udviklingen af et europæisk marked for de nye krypterede tjenester.

Et sådant initiativ ville endvidere være nyttigt inden for rammerne af informations-samfundet, hvor krypterede tjenester forventes at komme til at spille en afgørende rolle. Et EF-initiativ ville også have den fordel at fjerne fragmenteringen af det indre marked, og det vil samtidig kunne tilgodese andre fællesskabsmål, som f.eks. de industri- og kulturpolitiske og målene for forbrugerbeskyttelse.

De allerfleste operatører har udtrykt sig positivt om et EF-initiativ. I den henseende har European Digital Video Broadcasting (DVB) vedtaget en henstilling, hvori behovet for klare og ensartede retlige rammer i Unionen understreges. Dette krav blev i øvrigt støttet af Europa-Parlamentet, der foreslog at tilføje en betragtning i direktivet om standarder for transmission af tv-signaler, hvori det præciseres, at der er behov for en effektiv EF-lovgivning til bekæmpelse af piratvirksomhed; denne betragtning blev godkendt af Rådet, da det vedtog direktivet den 24. oktober 1995.

Kommissionen ønsker imidlertid, før den tager et initiativ, at få kendskab til de berørte parter holdning til nedenstående foranstaltning.

Kommissionen vil herefter kunne foreslå en foranstaltning til harmonisering af medlemsstaternes lovgivning. I betragtning af proportionalitets- og subsidiaritetsprincippet vil der i foranstaltningen kun blive foreskrevet en minimal harmonisering, således at medlemsstaterne får mulighed for at indføre strengere regler, samtidig med at der sikres en ensartet minimumsbeskyttelse i hele Unionen. Foranstaltningen vil ligeledes kunne forbyde fremstilling, salg, besiddelse både i handelsmæssig og privat sammenhæng, installation og salgsfremme af dekoderudstyr,

der giver adgang til krypterede tjenester uden krypteringsforetagendets tilladelse. Et sådant skridt ville kunne sikre en ensartet beskyttelse i Den Europæiske Union mod ulovlig modtagelse af krypterede tjenester og dermed give de berørte kredse retssikkerhed.

Den næste fase

Kommissionen ønsker en *åben høring* om grønbogen. Enhver person eller virksomhed, organisation eller myndighed kan svare. Der er tale om en tovejshøring, der ikke blot henvender sig til sammenslutninger eller brancheorganisationer, men også til alle individuelle operatører. Grønbogen vil blive fremsendt til Europa-Parlamentet, Det Økonomiske og Sociale Udvalg, Regionsudvalget, medlemsstaterne, Det Europæiske Økonomiske Samarbejdsområde samt landene i Central- og Østeuropa.

Fristen for indsendelse af bidrag er den 31. maj 1996. På grundlag af de modtagne bidrag vil Kommissionen i løbet af sommeren 1996 beslutte, om det er nødvendigt med et EF-initiativ.

Indledning

1. Problemet med ulovlig modtagelse

I de seneste år har kryptering af signaler i stadig højere grad været anvendt inden for radio- og tv-spredning. Siden 1980'erne er der dukket en række systemer op, der med forskelligt sikkerhedsniveau anvender en form for kryptering, hvorved originalbilledet eller originallyden ændres inden udsendelsen, således at en almindelig modtager ikke kan genskabe originaludsendelsen. Modtageren har derfor for at genskabe billedet behov for særligt dekoderudstyr (dekoder, smart-kort eller edb-program), der normalt leveres mod betaling af en licensafgift, og som kan aflæse de instruktioner, der sendes med det krypterede signal.

Denne teknologi, der oprindeligt blev anvendt af kabelnetdistributører for at modulere de kanaler, som modtagerne ifølge deres abonnement skulle have adgang til, bredte sig hurtigt til jordbaserede betalingskanaler, og den har på det seneste undergået en kraftig udvikling i forbindelse med udbredelsen af krypterede satellitbaserede kanaler. Den kraftigste udvikling i anvendelsen af kryptering vil imidlertid ske i forbindelse med den digitale teknik og udviklingen af informationsfundets tjenester, som f.eks. *interaktiv home-shopping, teleformidlede informationstjenester, erhvervslivets online-specialtjenester, interaktive spil osv., der alle i forskellig grad vil skulle krypteres, for at de kan blive rentable.*

Kryptering anvendes af flere grunde. Som led i en kommerciel strategi for at finde nye indtægtskilder, og for rettighedshavernes vedkommende for at beskytte og udnytte de programmer, der fremføres af signalet. Beskyttelse af mindreårige, bl.a. i forbindelse med radio- og tv-kanaler for voksne, kan ligeledes være en vigtig grund, ligesom muligheden for en bedre identifikation af markedet for at kunne "målrette" de salgsfremmende aktiviteter.

Parallelt med de officielle fabrikanter af dekoderudstyr har der imidlertid udviklet sig en blomstrende uautoriseret industri. Denne piratindustri fremstiller og sælger dekodere - normalt til priser under det godkendte udstyr - der gør det muligt at modtage de omhandlede tjenester uden udbyderens tilladelse.

Det anslås, at dette ulovlige dekoderudstyr i dag udgør mellem 5-20% af det samlede antal dekodere med en årlig omsætning på flere millioner ECU. På dette piratmarked er der endda dukket en fagpresse op med målrettede reklamer og oprettelse af særlige forhandlernet af dette ulovlige udstyr. Endvidere er der oprettet egentlige serviceafdelinger, der tilbyder vedligeholdelse og nogle gange endda udskiftning af udstyret, hvis operatøren skifter system.

Markedsføringen af dette ulovlige udstyr har først og fremmest negative følger for operatørerne af krypterede tjenester. De lider ikke blot tab (tabte potentielle markedsandele og indtægtstab); de påføres derudover ekstraomkostninger, da de er nødt til at indføre salgsordninger for dekoderudstyret (normalt udlejning), der er særdeles kostbare, for at kunne kontrollere anvendelsen af udstyret.

For programproducenterne medfører det ulovlige udstyr endvidere indtægtstab, idet de ved forhandlingen om vederlaget for afståelse af rettighederne, der bl.a. baseres på antal abonnenter på tjenesten, ikke har taget højde for de personer, der modtager programmet ved hjælp af ulovligt udstyr.

Hvad angår leverandørerne af teknologien, undergraver det ulovlige udstyr markedets tillid til deres system, og det medfører indtægtstab, da en del af det potentielle marked dækkes af ulovligt udstyr.

Endelig udgør salg af ulovligt udstyr en fare for forbrugerne, der kunne tage fejl af dets oprindelse og tro, at de køber autoriseret udstyr, mens der i virkeligheden er tale om en piratdekode. Hvis operatøren i det tilfælde af sikkerhedsgrunde ændrer krypteringssystemet, vil det købte udstyr ikke kunne hjælpe forbrugeren, der vil være nødt til for egen udgift at købe en anden dekode. Endvidere vil tjenesteudbyderne vælte det tab, de lider som følge af piratvirksomhed, over på salgs- eller udlejningsprisen for det lovlige udstyr, som forbrugerne køber.

II. Den lovgivningsmæssige situation

For at bringe denne situation til ophør har operatørerne krævet, at medlemsstaterne vedtager en særlovgivning, der sikrer en hurtig og effektiv retlig beskyttelse mod fremstilling og salg af ulovligt dekoderudstyr. Det er korrekt, at de teknologiske fremskridt har øget krypteringssystemernes sikkerhed, men rent tekniske løsninger har imidlertid ofte vist sig at være ineffektive. Operatørerne skal i deres valg af krypteringssystem tage højde for de omkostninger, der følger med systemet; således kan en høj sikkerhed, der samtidig er meget kostbar, vise sig at være økonomisk uholdbar. Samtidig viser erfaringen, at udviklingen af piratteknikker sker i samme takt som udviklingen af krypteringsteknikker, og selv i forbindelse med anvendelse af den digitale teknologi kan det ikke udelukkes, at de nye systemer vil blive angrebet. For at tage kampen op mod denne piratindustri, har det vist sig nødvendigt med lovgivningsmæssige indgreb, der kan supplere de teknologiske muligheder, og det har medført en bølge af lovgivningstiltag i medlemsstaterne, der endnu ikke er afsluttet, og som har haft helt forskellige udgangspunkter¹.

I den forbindelse annoncerede Kommissionen i sin meddelelse "Europa på vej mod informationssamfundet: en handlingsplan" fra juli 1994 (KOM(94) 347), at den ville udarbejde en "grøn bog om retlig beskyttelse af krypterede tjenester i det indre marked" for at undersøge de problemer, der opstår som følge af en manglende lovgivning om ulovlig modtagelse af krypterede tjenester i visse medlemsstater og forskellene i den eksisterende lovgivning i de øvrige medlemsstater.

III. De omfattede tjenester

Nedenstående analyse omhandler således ulovlig modtagelse af krypterede tjenester, dvs. modtagelse uden betaling og/eller uden tjenesteudbyderens tilladelse, samt den måde hvorpå medlemsstaterne ved lovgivning har forsøgt at løse dette problem. Ved

¹ Jf. kapitel 3: Lovgivningen i medlemsstaterne.

krypterede tjenester forstås tjenester, hvis signal er krypteret for at sikre betaling af licens. I denne kategori indgår traditionel krypteret radio- og tv-spredning (pr. kabel, radiokæder eller via satellit), de nye radio- og tv-spredningstjenester (digital-tv, pay-per-view, near video-on-demand), og informationssamfundets tjenester, dvs. teleformidlede tjenester, der bestilles af en modtager (f.eks. video-on-demand, bestillingsspil, elektronisk handel, multimedie-informationstjenester).

Kategorien udelukker derimod tjenester, der ikke er krypteret for at sikre betaling af en licensafgift. Det gælder f.eks. tjenester, der er krypteret for at sikre fortrolighed for de transmitterede meddelelser, dvs. finansielle tjenester eller telekommunikationstjenester (herunder mobiltelefoni, der anvender GSM-systemet). Disse tjenester er udelukket, fordi den almene interesse, der er på spil i tilfælde af aflytning, dvs. meddelelsens integritet og fortrolighed, er helt forskellig fra beskyttelse af en tjeneste, der ydes mod vederlag. Denne forskel har imidlertid både på nationalt og internationalt niveau fundet meget forskellige lovgivningsmæssige løsninger, især hvad angår foranstaltninger og sanktioner, som gør, at de to problemer ikke kan behandles samlet.

Grønbogen behandler heller ikke systemer, der forhindrer kopiering af værker og andre beskyttede frembringelser, der allerede er behandlet i en grøn bog om ophavsret i informationssamfundet, som Kommissionen vedtog i juli 1995.

Endelig omhandler grønbogen ikke standardisering af adgangsstyringssystemer og betingelserne for udstedelse af licens til disse systemer, der allerede er omfattet af direktivet om standarder for transmission af tv-signaler², og heller ikke spørgsmål vedrørende de nationale myndigheders kontrol med kodningssystemer. Sidstnævnte spørgsmål, der hænger nøje sammen med spørgsmålet om sikkerhed, behandles i øjeblikket af Kommissionen i forbindelse med arbejdet med informationssystemers sikkerhed. Det kan eventuelt blive nødvendigt at behandle det særskilt, hvis de nationale lovgivninger truer det indre markeds funktion.

IV. Det forberedende arbejde

Med henblik på udarbejdelsen af grønbogen har Kommissionen anmodet tre uafhængige firmaer om at undersøge de teknologiske, økonomiske og juridiske aspekter af markedet for krypterede tjenester³.

Den første undersøgelse ("Technical aspects related to encrypted broadcasts") behandler især de økonomiske og tekniske aspekter og omhandler bl.a. de nuværende krypteringssystemer, deres fordele og ulemper samt deres sårbarhed. De økonomiske

² Europa-Parlamentets og Rådets direktiv 95/47 af 24. oktober 1995 om standarder for transmission af tv-signaler (EFT L 281 af 23.11.1995, s. 51).

³ Disse undersøgelser beror hos Kommissionen og kan rekvireres på nedenstående adresse:
Europa-Kommissionen, Generaldirektorat XV - Det indre Marked og Finansielle Tjenesteydelser
Medier, kommerciel kommunikation og illoyal konkurrence
GD XV/E/5 C 107 8/59
Rue de la Loi 200
B-1049 Bruxelles
Fax: 32.2.295.77.12
E-mail: e5@dg15.cec.be

aspekter omhandler især omkostningerne i forbindelse med abonnentstyringsystemer, tendensen til udvikling af kompatible systemer samt de nye digitale teknologiers opdukken.

I den anden undersøgelse ("Protection of encrypted broadcasts") behandles de juridiske aspekter. Der er således foretaget en analyse af de faktorer, der har været afgørende for udviklingen af krypterede radio- og tv-spredningstjenester, årsagerne til piratvirksomhed samt en gennemgang af den lovgivning, der er indført for at dæmme op for denne virksomhed.

Den tredje undersøgelse ("Legal protection of encrypted broadcasting signals") indeholder en analyse af medlemsstaternes eksisterende lovgivning om beskyttelse af krypterede signaler samt domstolens anvendelse heraf og de eventuelle kontrolmekanismer og sanktioner, der er foreskrevet. Endvidere er der foretaget en analyse af de bestemmelser, der er vedtaget af de internationale organer (Europarådet, WIPO).

Endvidere iværksatte Kommissionen i marts 1995 en omfattende høring blandt de industrisektorer, der er berørt af problemerne med ulovlig modtagelse af krypterede tjenester, herunder radio- og tv-selskaber, fabrikanten af dekoderudstyr, kabel-distributører, programproducenter, telekommunikationsselskaber samt i øvrigt alle, der ønskede at deltage i en sådan høring.

Resultaterne af denne høring bekræftede, at ulovlig modtagelse af krypterede tjenester og forskellene i de nationale lovgivninger udgør et reelt problem for medieindustrien. Faktisk er det sådan, at når virksomheder inden for medieindustrien skal træffe beslutning om at sende en ny krypteret tjeneste i en medlemsstat, spiller muligheden for en effektiv beskyttelse mod ulovlig modtagelse en afgørende rolle. Hvis der ikke findes en sådan retlig beskyttelse, foretrækker operatørerne ofte at lade være med at markedsføre tjenesten.

Det store flertal af operatørerne går således ind for et EF-initiativ, og i den henseende har European Digital Video Broadcasting (DVB), der står bag standardiseringen af normer til digital-tv, inden for rammerne af sin ekspertgruppe om piratvirksomhed i forbindelse med krypterede tjenester, vedtaget en henstilling, hvori gruppen understreger behovet for klare og ensartede retlige rammer i Unionen, som man kan støtte sig til i tilfælde af ulovlig modtagelse af krypterede tjenester.

Dette krav blev støttet af Europa-Parlamentet, der i løbet af proceduren, der førte til vedtagelsen af direktivet om standarder for transmission af tv-signaler⁴, foreslog at tilføje en betragtning, hvori det præciseres, at med indførelsen af den digitale teknologi på det audiovisuelle område vil mulighederne for piratvirksomhed stige, hvilket vil få uheldige følger for operatører og programproducenter, og at det derfor bliver stadig mere påkrævet med en effektiv EF-lovgivning til bekæmpelse af piratvirksomhed; denne betragtning blev godkendt af Rådet, da det vedtog direktivet den 24. oktober 1995.

4

Ovennævnte direktiv 95/47.

KAPITEL 1: DET EUROPÆISKE MARKED FOR KRYPTEREDE TJENESTER

1. Et marked i hastig udvikling

I de seneste år har den *teknologiske udvikling* (f.eks. anvendelse af satellitter og lyslederkabler) medført en hurtig ændring af det audiovisuelle landskab i Europa og gjort det muligt til stadighed at øge udbuddet af tjenester. Da et stigende antal operatører anvender *målrettede kommercielle strategier*, har kryptering af signaler vist sig at være af afgørende betydning for tjenesternes rentabilitet.

Den traditionelle finansiering af private kanaler, der udelukkende er baseret på reklameindtægter, er ofte utilstrækkelig for de nye operatører. Med den gradvise stigning i udbuddet af radio- og tv-kanaler, vil de traditionelle annoncørers bidrag pr. kanal falde. Samtidig forsøger operatørerne at profilere sig i forhold til det stigende antal potentielle konkurrenter ved at opfylde særlige behov på *nichemarkeder* i forhold til modtagernes smag og interesser (film-, musik- og sportskanaler). Således adskiller operatøren sig fra sine konkurrenter på massekommunikationsmarkedet ved målrettet at dække denne hidtil udækkede eller dårligt dækkede efterspørgsel. Hvis man imidlertid sammenligner identiske geografiske områder, vil modtagerne af en nichetjeneste nødvendigvis udgøre en udvalgt målgruppe, og der vil være færre modtagere. Operatørerne kan derfor ikke regne med reklameindtægter fra annoncører⁵ på massekommunikationsmarkedet, idet de er mindre interesseret i en strategi, der ikke henvender sig til det brede publikum.

1.1. Begrundelsen for at anvende kryptering

De væsentligste grunde til at anvende kryptering af signaler kan resumeres som følger:

- *Behov for at sikre, at modtagerne er med til at finansiere tjenesterne:* Begrebet målrettet tjeneste er baseret på muligheden af at tilbyde en vis modtagergruppe noget ekstra ud over de tjenester, der henvender sig til det brede publikum. Det vil derfor være nødvendigt, at modtagerne bidrager ved finansieringen af de omhandlede tjenester, og at ikke-abonnenter takket være kryptering udelukkes fra modtagelse.
- *Mulighed for at øge reklameindtægterne pr. modtagerenhed:* Ved at kryptere signalet vil operatøren bedre kunne sælge reklameplads eller sikre program-sponsorering hos de virksomheder, der er interesseret i disse nichemarkeder. I det tilfælde betaler annoncørerne ikke længere for et helt geografisk marked, men udelukkende for det udvalgte segment. De vil derfor være parat til at betale en højere pris pr. modtagerenhed, idet kvaliteten heraf anses for at være højere end massemediernes modtagerskare.

5

I dette dokument omfatter termen "annoncør" "virksomheder, der anvender kommerciel kommunikation". Termen omfatter alle former for reklame, salgsfremme, direkte marketing, sponsorering og PR. Overbegrebet "annoncør" er valgt for at tage højde for udviklingen i brugen af marketingstrategier som følge af udviklingen på medieområdet.

- *Mulighed for bedre at målrette udbuddet:* Et bedre kendskab til modtageren af tjenesten vil gøre det nemmere for operatøren at tilbyde en tjeneste, der er skræddersyet til målmarkedets efterspørgsel.
- *Forenklet erhvervelse af rettigheder til radio- og tv-spredning:* Spredning via satellit har udvidet det potentielle modtagerområde betragteligt. Erhvervelse af rettigheder til radio- og tv-spredning sker imidlertid stadig på territorielt grundlag, hvilket indebærer, at modtagelsen begrænses til et geografisk eller sprogligt område. Takket være kryptering vil operatøren kunne begrænse modtagelsen af signalet udelukkende til de områder, der har erhvervet de nødvendige rettigheder. Endvidere vil kryptering, således som nævnt i "kabel og satellit"-direktivet⁶, gøre det muligt i forbindelse med erhvervelse af rettigheder til udsendelse via satellit og viderespredning pr. kabel at tage den faktiske modtagergruppe i betragtning (f.eks. antal abonnenter og ikke geografisk område), hvilket vil gøre det billigere at indkøbe programmer til en nichetjeneste.
- *Tilføjelse af yderligere en fase i spredningsprocessen:* Krypteret udsendelse af programmer gør det muligt for rettighedshaverne at tilføje yderligere en fase i spredningsprocessen. Operatører af en krypteret tjeneste udsender ofte værkerne, før de udsendes for den brede offentlighed, og de er normalt parate til at betale store beløb for denne enerettighed. Rettighedshaverne vil således få en ekstra indtægtskilde.
- *Lovgivningsmæssige krav:* Af sociale grunde, herunder bl.a. *beskyttelse af mindreårige* (f.eks. i forbindelse med radio- og tv-kanaler, der henvender sig til et voksent publikum), kan myndighederne, således som foreskrevet i direktivet om fjernsyn uden grænser⁷ (artikel 22, andet punktum), tillade sådanne tjenester, hvis de krypteres, således at modtagelsen begrænses til visse seerkategorier.

1.2. Krypterede tjenester

I dag består det europæiske marked for krypterede tjenester væsentligst af betalings-tv-kanaler⁸. Denne tjeneste, der i begyndelsen blev udsendt via kabel eller radiobølger, har især udviklet sig med indførelsen af direkte modtagelse via kommunikationssatellitter med mellemstor og stor sendeeffekt, der gør det muligt at modtage en udsendelse overalt inden for satellittens dækningsområde ved hjælp af en parabolantenne.

⁶ Rådets direktiv 93/83 af 27. september 1993 om samordning af visse bestemmelser vedrørende ophavsrettigheder og ophavsretsbeslægtede rettigheder i forbindelse med radio- og tv-udsendelse via satellit og viderespredning pr. kabel (EFT L 248 af 6.10.1993, s. 15).

⁷ Rådets direktiv 89/552 af 3.10.1989 om samordning af visse love og administrative bestemmelser i medlemsstaterne vedrørende udøvelse af tv-radiospredningsvirksomhed (EFT L 298 af 17.10.1989, s. 23).

⁸ Termen "betalings-tv" indebærer, at seeren skal betale for at modtage en bestemt kanal, der transmitteres via radiokæde, kabel eller satellit.

Den teknologiske udvikling har imidlertid gjort det muligt at lancere mere sofistikerede betalingstjenester, som f.eks. *pay-per-view-tjenester*⁹, der betyder, at seeren betaler for at modtage visse programmer. Pay-per-view er teknisk muligt selv uden digital kompression, men systemet kræver imidlertid et sofistikeret abonnentstyringssystem. Pay-per-view betyder, at seeren betaler for en bestemt begivenhed (f.eks. en koncert eller en boksekamp) eller for en række begivenheder (f.eks. retten til at se 10 fodboldkampe). I sidstnævnte tilfælde er radio- og tv-selskabet ikke på nuværende tidspunkt i stand til at identificere de begivenheder, som seeren har modtaget. Man er imidlertid ved at udvikle systemer, der i fremtiden vil gøre det muligt at sikre en bedre vederlagsbetaling til rettighedshaverne i forhold til det faktiske "forbrug" af deres programmer.

Den næste fase forventes at blive *near-video-on-demand*, der indebærer, at radio- og tv-selskabet altid sender det samme program (generelt, men ikke nødvendigvis, en film) på forskellige tidspunkter. Modtageren kan således ikke blot vælge program, men også inden for visse grænser, tidspunkt. Denne fase vil blive efterfulgt af ægte *video-on-demand*, der vil give modtageren en større frihed hvad angår filmens begyndelsestidspunkt, som ikke længere fastsættes af radio- og tv-selskabet.

Den eksplosive vækst i anvendelsen af kryptering vil imidlertid først ske med udviklingen af informationssamfundets øvrige tjenester. Ikke blot de traditionelle audiovisuelle tjenester, men også andre anvendelser, som f.eks. *interaktiv home-shopping*, *teleformidlede informationstjenester*, *online-specialtjenester*, *interaktive spil osv.*, vil i forskellig grad skulle baseres på kryptering for at blive rentable. Da kryptering endvidere ofte vil være nødvendig af sikkerhedsgrunde (f.eks. elektronisk betaling i forbindelse med home-shopping), vil et samspil mellem disse to krypteringsanvendelser (abonnentsystemet, der øger sikkerhedskontrollen) - på betingelse af at der hersker retssikkerhed på området - kunne gøre anvendelsen af kryptering yderst relevant for at fremme udviklingen af alle de omhandlede tjenester i informationssamfundet.

Udviklingen af disse nye tjenester forudsætter imidlertid i vidt omfang, at der indføres en retlig ramme, der både tager højde for operatørernes og tjenestemodtagernes legitime krav. Det er i den forbindelse altafgørende, hvorledes man på verdensplan løser de forskellige sikkerhedsproblemer, som anvendelsen af elektroniske transaktioner giver anledning til, herunder de lovgivningsmæssige grænser for anvendelse af krypteringssystemer, offentlige myndigheders kontrol med krypterede meddelelser af nationale sikkerhedsgrunde samt parternes identifikation og ægthed. Kommissionen er i forbindelse med sine aktiviteter vedrørende informationssystemernes sikkerhed ved at undersøge, om det er relevant på europæisk niveau at oprette nogle organisationer, der helt uafhængig af de offentlige myndigheder kunne tillægges kontrol- og godkendelsesfunktioner.

⁹

I USA er 35% af de kabeltilsluttede husstande (ca. 20 000 000) udstyret til at modtage disse tjenester. I Frankrig tilbyder Multivision-tjenesten to pay-per-view-kanaler til 220 000 husstande.

2. Et europæisk marked

Der er i dag i Europa 180 tv-kanaler, der sender via 27 satellitter¹⁰, og en stor del af disse anvender mere eller mindre sofistikerede former for kryptering (tabel 1). Mange af dem er tematiske kanaler (f.eks. programmer for børn, sports- og filmkanaler osv.).

Tabel 1: Antal abonnenter på de største betalings-tv-kanaler (i 1 000):¹¹

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

I fremtiden må man forvente en kraftig vækst i udbuddet af krypterede tjenester i Europa. Opsendelsen af de nye helt digitale satellitter (som f.eks. Astra 1e og 1f) og udbredelsen af lysledernet vil betyde, at de operatører, der allerede er på markedet, vil kunne øge deres udbud. I den henseende har flere operatører i pressen bekendtgjort, at de har planer om at lancere programpakker af digital-tv. F.eks. vil Nethold-koncernen, der kontrollerer Filmnet, snart lancere en pakke på 150 digitale kanaler, hvoraf 50 tilbyder pay-per-view-film. Som et første skridt mod lanceringen af ægte video-on-demand-tjenester planlægger BSKyB at lancere 16-32 pay-per-view-kanaler ved udgangen af 1996. Canal+udbyder snart en pakke på over 20 digitale kanaler. Tjenesten vil, ud over de nuværende tjenester, indeholde pay-per-view, videospil og digitale radiotjenester. Endvidere vil en række franske kanaler, herunder TF1, Arte og La 5^e gå sammen om i 1996 at lancere en programpakke af digital-tv fra samme satellit. Endelig vil TF1 udbyde en tjenestepakke, lige fra video-on-demand til interaktive programmer fra 5 transpondere i Eutelsat.

¹⁰ Det europæiske observatorium for det audiovisuelle område: "Annuaire Statistique. Cinéma, télévision, vidéo et nouveaux médias en Europe", 1994-1995, Strasbourg 1994.

¹¹ Det europæiske observatorium for det audiovisuelle område: "Annuaire Statistique. Cinéma, télévision, vidéo et nouveaux médias en Europe", 1994-1995, Strasbourg 1994 og Libération: "Les comptes décryptés de Canal+". L'événement, 4.11.1994.

Herudover vil nye operatører dukke op på markedet for informationssamfundets tjenester. Det vil bl.a. være tilfældet for selskaber inden for telekommunikation. F.eks. har British Telecom allerede iværksat et pilotprojekt, der omfatter 2 500 husstande, der har adgang til tjenester som interaktiv home-shopping, video-on-demand, videospil osv.

Hidtil har de fleste kanaler dækket et bestemt sprogligt og geografisk område. Det er ikke desto mindre klart, at de nationale markeder i fremtiden ofte vil være for begrænsede, og behovet for nemt at kunne overskride grænserne mellem medlemsstaterne vil stige. Dette kan tilskrives følgende faktorer:

- *Med det stigende antal krypterede tjenester vil operatørerne skulle udbyde stadig mere målrettede tjenester for at opfylde markedets krav. Da denne efterspørgsel hidtil ikke har været tilfredsstillende, kan der opstå et nichemarked for en del af befolkningen, der er parat til at betale for denne merværdi. Med det stigende udbud af ukodede generelle tjenester, har de kodede tjenester udviklet sig for at tilfredsstille en stadig mere specialiseret efterspørgsel, hvilket har gjort det nødvendigt, at den endelige modtager betaler et vederlag. Udviklingen af sådanne målrettede levedygtige tjenester kræver imidlertid et marked af en vis størrelse, og da markedet for en nichetjeneste sammenlignet med tilsvarende geografiske områder er mindre end markedet for massemedietjenester, er det ofte kun rentabelt, hvis det geografiske marked er større.*
- *Mulighed for bedre at opfylde de sproglige og kulturelle behov. Den nye teknologi betyder, at én og samme kanal kan udsende på forskellige sprog samtidig på forskellige lydbånd. Endvidere vil strategien for de interaktive tjenester i stadig højere grad blive baseret på specialtjenester og/eller levering af tjenestepakker. Førstnævnte vil ofte imødekomme den grænseoverskridende nicheefterspørgsel og vil derfor være baseret på andre faktorer end den nationale kultur, og den anden vil give modtageren mulighed for selv at vælge, hvad han vil se. Med udbredelsen af den avancerede informationsteknologi, vil udbyderen således kunne tilbyde en meget bred vifte af tjenester og lade film/programmer eller andre tjenester, der afspejler de nationale forskelle, indgå i pakken.*
- *Udviklingen af teknologiske applikationer. Den konstante forbedring og den fortsatte integration af de audiovisuelle tjenesters distributionssystemer, der er mulig takket være den kommercielle anvendelse af den nye teknologi (transmission via satellit, lysledere, udvikling af ISDN (Integrated Services Digital Network) på europæisk niveau for at nå det integrerede bredbåndsnet (Integrated Broadband Communication networks), gør disse tjenester mere og mere uafhængige af afstanden mellem udbyderen og den endelige modtager.*
- *De lovgivningsmæssige tiltag, der sigter mod *gradvis liberalisering* af tele-tjenester (bl.a. via satellit og pr. kabel), og *harmoniseringen* af de grænseoverskridende regler for transport af signaler (bl.a. radio- og tv-spredning) i Europa (bl.a. hvad angår udsendelsernes indhold og ophavsret) er først nu begyndt at få positive følger for den frie udveksling af eksisterende audiovisuelle tjenester og tjenester under udvikling, hvoraf en stadig større del vil blive udbudt i krypteret form.*

- *Udviklingen i praksis ved tildeling af spredningsrettigheder:* På nuværende tidspunkt er det kun en begrænset del af de krypterede kanaler, der kan sendes internationalt, på grund af den traditionelle nationale praksis i forbindelse med tildeling af spredningsrettigheder. Ved hjælp af kryptering vil det i fremtiden være muligt at tildele spredningsrettigheder i forhold til den egentlige modtagergruppe og ikke blot i forhold til de nationale grænser.
- *Maksimal udnyttelse af transponderudgifterne:* Da transponderudgifterne er store, er det mere økonomisk for operatøren at udbyde sin tjeneste på så mange områder som muligt inden for satellittens dækningsområde.

Den udvikling, som disse tjenester undergår for at opfylde de stigende behov på de grænseoverskridende markeder, kan imidlertid bringes i fare på grund af et problem, der er alvorligt på europæisk niveau: nemlig piratvirksomhed.

3. Et marked, der er udsat for piratvirksomhed

3.1. Teknologiens udvikling

Ved hjælp af de avancerede teknologier er det i teorien i dag muligt at anvende et adgangsstyringssystem, der ville give et så højt sikkerhedsniveau, at al piratvirksomhed på forhånd måtte opgives. I praksis stilles der imidlertid også økonomiske og lovgivningsmæssige krav til disse systemer, dvs.:

- De skal fremstilles og distribueres til *rimelige priser*, da forbrugeren kun vil være indstillet på at betale et vist beløb for en dekoder¹² afhængig af programmernes interesse eller sammensætningen af kanaler, der kan nedtages med systemet.
- *Driftsomkostningerne* må ikke overstige de indtægter, der er usikre, dvs. de indtægter, der kan gå tabt på grund af salg af ulovligt udstyr.
- De skal overholde den *lovgivning*, som nogle medlemsstater har indført for anvendelse af kryptering i kommercielt øjemed.

Kravet om et acceptabelt omkostningsniveau i forbindelse med adgangsstyringssystemet gør det imidlertid umuligt at nå en fuldstændig sikkerhed mod ulovlig modtagelse. Fabrikkerne af ulovligt dekoderudstyr har draget fordel af dette forhold, og de følger nu blot den tekniske udvikling.

Systemernes udvikling afspejler denne situation. *Det mest enkle adgangsstyringssystem* består i en kryptering af de synkroniseringsimpulser, der indgår i radio- og tv-spredningssignalerne, således at en almindelig modtager ikke kan genskabe de vertikale og horisontale blokke. Billedet transmitteres normalt, men da der mangler synkroniseringsimpulser, viser skærmen kun en række billedkomponenter. Den information, der er nødvendig for at genskabe synkroniseringen sendes i ændret form (algoritme), der kan

¹²

Nogle krypteringsforetagender har valgt at leje dekoderudstyret til abonnenterne i stedet for at lade dem købe det. Dette giver mulighed for rimelige priser og sikrer samtidig, at udstyret tilbageleveres, når abonnementet udløber.

opfanges ved hjælp af dekoderudstyr, som kan genskabe de nødvendige synkroniseringsimpulser. Dette system har allerede i høj grad været udsat for piratvirksomhed¹³.

Andengenerationssystemerne fungerer lidt anderledes. To krypteringssystemer er blevet meget almindelige, nemlig:

- i "klip-og-rotér"-metoden bliver linjerne på deres plads, men de afbrydes tilfældigt og afslutningerne byttes om
- i "linjeombytnings"-metoden genskabes de linjer, der udgør billedet, i en fuldstændig anden orden. Denne metode er mere effektiv, men også dyrere end den førstnævnte, idet den kræver, at der lagres et større antal informationer i dekoderen.

Den store fordel ved de to systemer er, at de fuldstændig ødelægger billedstrukturen. Endvidere kan de anvendes sammen med et "smart-kort", der er en slags chip, der "læser" signalet ved indgangen og i samspil med dekoderen giver de informationer, der er nødvendige for at foretage dekryptering. Til denne generation hører de tre krypteringssystemer, der i øjeblikket er de mest anvendte i Europa, nemlig Videocrypt, Syster og Eurocrypt.

Forskningen i systemer, der giver endnu større sikkerhed, fortsætter imidlertid. Da den digitale teknik til radio- og tv-spredning i fremtiden vil blive anvendt til teletjenester og audiovisuelle tjenester, vil det være muligt at udvikle stadig mere sofistikerede og sikre krypteringssystemer. Faktisk er omsætningen af indholdet til digitale bit allerede i sig selv en slags kodning¹⁴.

Endvidere vil dekodere for at muliggøre indførelse af interaktive tjenester med tiden udvikle sig til "set top boxes", dvs. egentlige computere, der styres af et chipkort, som gør det muligt samtidig at identificere brugeren og aktivere krypteringsfunktionerne ved indgangen og udgangen. Dette udstyr gør det således muligt at modtage signalet, dekryptere det, eventuelt ændre indholdet og indlæse det på et andet medie, lagre det og printe det. Endvidere vil udstyret kunne interagere med det traditionelle udstyr (båndoptagere, computere, CD-afspillere og de nye videodiske) og sende et krypteret signal tilbage til operatøren, eventuelt med fortrolige finansielle data, med henblik på behandling af anmodningen.

3.2. Følgerne af piratvirksomhed

Fremstilling og salg af dekoderudstyr, der ikke er godkendt af krypteringsforetagendet, samt manipulering af lovligt udstyr for at kunne modtage en tjeneste f.eks. i længere tid end abonnementsperioden og modtage flere kanaler end godkendt af krypterings-

¹³ Det formodes, at piraterne genskaber synkroniseringsinformationen ved at kontrollere udgangspunktet for de på hinanden følgende billedlinjer. Den tekniske udformning af en dekoder blev endda for nogle år siden vist i den franske presse.

¹⁴ Den standardisering af krypteringssystemer til digital radio- og tv-spredning, der er sket i forbindelse med det arbejde, der er udført af Digital Video Broadcasting (DVB), er et afgørende skridt til udbredelse af krypteringsteknikkerne og et øget sikkerhedsniveau.

foretagendet, er i dag i nogle medlemsstater en særdeles rentabel aktivitet¹⁵. Det har i øvrigt i disse medlemsstater medført parallelle aktiviteter, som f.eks. udgivelse af særlige tidsskrifter og oprettelse af serviceafdelinger.

Disse aktiviteter, der muliggør ulovlig modtagelse af krypterede tjenester, har flere negative følger:

- krypteringsforetagenderne berøves indtægter, som de ville have fået, hvis modtageren havde købt autoriseret udstyr (ca. 200-250 ECU om året pr. ulovlig modtager)
- i nogle tilfælde vil det være nødvendigt at udskifte det system, der har været udsat for piratvirksomhed. Hvert år bruger operatørerne betydelige beløb (undersøgelsen foretaget hos operatørerne viste beløb fra ca. 60 000 ECU til over 1 200 000 ECU om året pr. operatør) for at sikre beskyttelse af deres systemer (kontrol med distributionen, forbedring af systemet, ændring af kortene osv.). Selv kontrolsystemet med smart-kort, der om noget synes uangribeligt, har vist sig at kunne brydes. Man kunne tro, at det i tilfælde af piratangreb ville være tilstrækkeligt at udskifte smart-kortet for at redde systemet. Men når der er mange abonnenter, kan omkostningerne til udskiftning af kortet bringe virksomhedens overskud alvorligt i fare. Ud over omkostningerne til selve smart-kortet¹⁶, skal man tage højde for omkostningerne til at udvikle det nye system samt kommunikations- og forsendelsesomkostningerne (undersøgelsen viste, at der kunne være tale om beløb på over 45 000 000 ECU for at gøre de piratangrebne systemer fuldstændig sikre på ny)
- det kræver tid at udvikle et nyt system. Hvis man igen anvender eksemplet med smart-kort, vil det, hvis en kanal skal udskifte kortene, kræve en vis tid at udvikle et nyt kort. I mellemtiden vil den eneste mulighed være at anvende en række midlertidige elektroniske modforholdsregler, indtil der kan komme et nyt kort på markedet; det er en farlig situation, idet piraterne foregriber disse modforholdsregler og fremstiller kort, der fungerer i ventetiden. Endvidere vil der altid være en overlappingsperiode, i hvilken det gamle og det nye system vil fungere samtidig. Det betyder, at de piratkort, der allerede er i omløb, også fortsat vil kunne anvendes, og det giver piraterne tid til at fremstille nye kort. Piraterne, der støttes af private investorer, kan faktisk allerede nu fremstille deres egne kort og chips næsten lige så hurtigt som radio- og tv-selskaberne. Andre teknikker til at sætte piraterne ud af spillet (som f.eks. udsendelse af desaktiveringssignaler, der kun annullerer ulovlige kort) har kun haft begrænset levetid (da piratindustrien fremstiller særligt udstyr til at blokere desaktiveringsbølgen)
- det medfører krænkelse af de formuerettigheder, som indehaverne af rettighederne til de programmer, der indgår i udsendelsen, har. Da rettighedshavernes vederlag normalt også tager højde for de potentielle modtagere, vil modtagelse af krypterede udsendelser ved hjælp af ulovligt udstyr betyde, at de unddrages de abonnementsindtægter, som de ville have modtaget,

15

Det anslås, at uautoriseret dekoderudstyr i dag udgør 5-20% af det samlede marked.

16

Ca. 5-25 ECU.

hvis indehaverne af dette udstyr i stedet havde købt en lovlig dekoder. Endvidere vil rettighedshaverne i forbindelse med forhandling om rettigheder til senere (ukodede) udsendelser have vanskeligere ved at opnå et rimeligt vederlag på grund af den ulovlige modtagelse, der allerede har fundet sted i forbindelse med udsendelsen på den krypterede kanal.

- indtægtstab og manglende tillid til *leverandørerne af teknologi*. Når der skal vælges krypteringssystem, ønsker operatørerne vistnok, at det valgte system er det mest sikre, således at de kan garantere rettighedshaverne, at de udsendelser, som de har givet tilladelse til, ikke udsættes for piratvirksomhed. Hvis der findes en høj procent ulovligt dekoderudstyr i handelen, vil det kunne tolkes som et udtryk for et ikke særlig effektivt system.
- det kan ødelægge *markedets tillid* til systemet. Markedet skal have tillid til kryptering, for at man kan fastholde den enerettighed, der er knyttet til disse tjenester, og for at man kan begrunde den yderligere fase i spredningsprocessen, og ulovlig modtagelse truer denne tillid. Rettighedshaverne vil tøve med at tillade de første udsendelser, radio- og tv-selskaberne vil ikke være indstillet på at betale særlig høje beløb, og forbrugerne vil ikke være indstillet på at betale licens.
- Endelig udgør salg af ulovligt udstyr en fare for *forbrugerne*, der kunne tage fejl af dets oprindelse og tro, at de køber autoriseret udstyr, mens der i virkeligheden er tale om en piratdekoder. Hvis operatøren i det tilfælde af sikkerhedsgrunde ændrer krypteringssystemet, vil det købte udstyr ikke kunne hjælpe forbrugeren, der vil være nødt til for egen udgift at købe en anden dekoder. Endvidere vil tjenesteudbyderne vælte det tab, de lider som følge af piratvirksomhed, over på salgs- eller udlejningsprisen for det lovlige udstyr, som forbrugerne køber.

Til disse direkte følger skal man tilføje de indirekte følger for udviklingen af markedet for krypterede tjenester. Markedet vil kun kunne udvikle sig, hvis der garanteres et passende sikkerhedsniveau. I modsat fald vil operatørerne tøve med at lancere aktiviteter, der kræver så store førstegangsinvesteringer.

4. Et marked med forskellig lovgivning

For at komme piratindustrien til livs har det vist sig nødvendigt med en lovgivningsmæssig løsning som supplement til de tekniske løsninger, og dette har fremkaldt en lovgivningsbølge i medlemsstaterne, der endnu ikke er afsluttet, og som har haft meget forskellige udgangspunkter. Denne lovgivning vil blive gennemgået i kapitel 3.

En sådan *lovgivningsmæssig forskel* kan imidlertid, afhængig af hvilken mediesektor der er tale om, medføre vanskeligheder for udviklingen af krypterede tjenester på europæisk niveau og true det indre markeds funktion. Da den tværnationale dimension bliver mere og mere nødvendig for udviklingen af en egentlig europæisk industri for krypterede tjenester, kan en manglende retlig beskyttelse mod piratvirksomhed få negative følger for udviklingen af disse tjenester på europæisk niveau.

Det blev således bekræftet under høringen, at en manglende retlig beskyttelse i et eller flere modtagerlande vil kunne få operatørerne til at beslutte ikke at dække en given

medlemsstat af frygt for følgerne af piratvirksomhed. En effektiv retlig beskyttelse er en afgørende faktor for at få en operatør til at markedsføre sin tjeneste i en medlemsstat.

De omkostninger, der opstår i forbindelse med afklaring af gældende national lovgivning og eventuelle søgsmål på grund af piratvirksomhed i de forskellige medlemsstater, betyder ekstraomkostninger for operatørerne, og deres aktiviteter bliver mere kostbare. Det vil ligeledes kunne få negative følger for udviklingen af tjenesterne.

I forbindelse med forhandling om rettigheder til programmerne, vil en forskellig retlig beskyttelse i samtlige medlemsstater gøre det vanskeligere at erhverve disse rettigheder, idet (især hvad angår nylige produktioner) operatørerne ikke kan garantere, at der ikke vil finde ulovlig modtagelse sted i de øvrige medlemsstater. Fastsættelse af vederlag til rettighedshaverne vil også blive vanskeligere, da man ikke med sikkerhed kan vurdere antal modtagere i hele signalets dækningsområde. Det bliver derfor vanskeligere for operatørerne at købe rettighederne til rimelige priser, hvilket vil afspejle sig i deres aktiviteter, herunder de tværnationale.

Da nogle former for transmission er mere udsat for ulovlig modtagelse end andre (bl.a. transmission via radiokæder og transmission via satellit i forhold til transmission pr. kabel, der normalt er sikrere på grund af den fysiske opkobling til modtageren), vil operatørerne kunne beslutte ikke at anvende visse af disse former på grund af den store fare for piratvirksomhed. Hvis der ikke findes en effektiv retlig beskyttelse, vil nogle systemer, herunder de systemer der er bedst egnet til tværnational transmission, risikere at blive mindre udbredt end andre.

En uensartet retlig beskyttelse i medlemsstaterne vil endvidere få betydning i tilfælde af import af ulovligt dekoderudstyr fra tredjelande. Faktisk vil sådant udstyr kunne komme ind i Fællesskabet via en medlemsstat, hvor det ikke er forbudt at markedsføre og distribuere ulovligt udstyr, og udstyret vil derefter nemt kunne komme ind i en anden medlemsstat. Bekæmpelsen af ulovlig modtagelse i sidstnævnte medlemsstat kan således blive særdeles ineffektiv.

Forskellig lovgivning om ulovlig modtagelse vil endvidere medføre konkurrenceforvriddning for operatørerne i de forskellige lande. De operatører, der transmitterer signaler i medlemsstater, der har en effektiv retlig beskyttelse, vil få konkurrencefordele (der f.eks. vil afspejle sig i deres mulighed for at købe programmer) i forhold til de operatører, der transmitterer signaler i en medlemsstat, hvor der ikke findes en retlig beskyttelse, idet sidstnævnte vil få ekstraomkostninger, da de f.eks. er nødt til at anvende et ekstra sikkert krypteringssystem.

Endelig vil forskellig lovgivning i medlemsstaterne betyde, at de muligheder, som direktivet om standarder for transmission af tv-signaler¹⁷ giver, risikerer at falde til jorden. Anvendelsen af stadig mere standardiserede systemer vil nemlig blive vanskeliggjort af en uensartet retlig beskyttelse mod ulovlig modtagelse i medlemsstaterne. Sikkerhedsniveauet for systemet og mulighederne for distribution af dekoderudstyr vil variere afhængig af modtagerland, hvilket vil medføre en ny fragmentering af det audiovisuelle område, der i en vis grad skulle være standardiseret.

17

Direktiv 95/47 nævnt ovenfor.

European Digital Video Broadcasting (DVB), som står bag standardiseringen af normerne for digital-tv, der i et vist omfang genfindes i direktiv 95/47, har inden for rammerne af sin ekspertgruppe om piratvirksomhed i forbindelse krypterede tjenester vedtaget en henstilling, i hvilken den understreger nødvendigheden af, at operatørerne får en klar og ensartet retlig ramme på europæisk niveau, som de kan støtte sig til i tilfælde af ulovlig modtagelse af krypterede tjenester.

KAPITEL 2: DE INTERNATIONALE REGLER

1. Arbejdet i Europarådet

Europarådet vedtog i september 1991 en henstilling til medlemsstaterne om *retlig beskyttelse af krypterede fjernsynsprogrammer*¹⁸. Denne henstilling er blevet ajourført af en anden henstilling om foranstaltninger mod piratvirksomhed på fonogram- og videogramområdet, der blev vedtaget i januar 1995¹⁹.

I præamblen understreger Europarådet fordelene ved indførelsen af betalings-tv, bl.a. for produktionen af audiovisuelle værker. Rådet understreger, at krypterede radio- og tv-tjenester giver mulighed for et bredere programudbud til offentligheden, øger udnyttelsesmulighederne for beskyttede værker og bidrager til at finansiere produktionen af værker og programmer i Europa takket være den nye finansiering, som kryptering sikrer kanalerne.

Derefter fremhæves de negative følger af ulovlig adgang til krypterede radio- og tv-spredningstjenester og de aktiviteter, der bør være ulovlige, opremses. Der er bl.a. tale om:

- fremstilling af dekoderudstyr med det formål at give adgang til krypterede tjenester for personer, der falder uden for krypteringsforetagendets målgruppe
- indførsel af dekoderudstyr med det formål at give adgang til krypterede tjenester for personer, der falder uden for krypteringsforetagendets målgruppe
- distribution af dekoderudstyr med det formål at give adgang til krypterede tjenester for personer, der falder uden for krypteringsforetagendets målgruppe
- salgsfremme og reklame for fremstilling, indførsel og distribution af det ovenfor nævnte dekoderudstyr
- besiddelse i erhvervsmæssigt øjemed af dekoderudstyr, der giver adgang til krypterede tjenester for personer, der falder uden for krypteringsforetagendets målgruppe.

Medlemsstaterne kan bestemme, at besiddelse til privat brug også skal betragtes som en ulovlig aktivitet.

I henstillingen defineres herefter *krypterede tjenester* som alle tv-tjenester, uanset på hvilken måde de transmitteres eller retransmitteres, hvis karakteristika er ændret for at begrænse modtagelsen til en bestemt gruppe. Endvidere understreger Rådet i begrun-

¹⁸ Ministerkomitéens henstilling nr. R (91) 14 til medlemsstaterne om retlig beskyttelse af krypterede fjernsynsprogrammer (Recommendation No R (91) 14 of the Committee of Ministers to Member States on the legal protection of encrypted television services).

¹⁹ Ministerkomitéens henstilling nr. R (95) 1 til medlemsstaterne om foranstaltninger mod piratvirksomhed på fonogram- og videogramområdet (Recommendation No R (95) 1 of the Committee of Ministers to the Member States on measures against sound and audiovisual piracy).

delsen, at denne definition (og den beskyttelse, der følger deraf) gælder alle foretagender, der udbyder krypterede tjenester, uanset om det er på lokalt, regionalt, nationalt eller tværnationalt niveau uden hensyntagen til udsendelsens oprindelsesland.

Den beskyttelse, som Europarådet anbefaler, forudsætter ingen gensidighed. Rådet understreger således også i begrundelsen, at udelukkelse af tjenester fra andre medlemslande, vil kunne skabe problemer for de tjenester, der har oprindelse i modtagerlandet.

Dekoderudstyr defineres i henstillingen som apparater, udstyr eller andre anordninger, der helt eller delvis er specielt fremstillet eller tilpasset for at muliggøre adgang til dekryptering af en krypteret tjeneste, dvs. uden at ændre tjenestens karakteristika²⁰.

Endelig defineres distribution som salg, udlejning eller kommerciel installation af dekodeudstyr, samt besiddelse af dekodeudstyr for at udføre disse aktiviteter. Denne definition dækker udelukkende kommercielle aktiviteter og ikke private.

Hvad angår sanktioner opfordres medlemsstaterne i henstillingen kraftigt til at indføre strafferetlige eller administrative sanktioner for den ovennævnte adfærd, dog med én undtagelse. Salgsfremme og reklame for fremstilling, indførsel og distribution af ulovligt dekodeudstyr giver ikke anledning til strafferetlige eller administrative sanktioner²¹.

De civilretlige afhjælpningsmuligheder, der foreslås i henstillingen, omfatter ud over de strafferetlige sanktioner, mulighed for at krypteringsforetagenderne anlægge sag med krav om erstatning eller del i fortjenesten.

De personer, der har ophavsretten til de programmer, der er indeholdt i tjenesterne, har ikke søgsmålsret. Europarådet anfører i begrundelsen, at selv om de personer, der har ophavsretten til de programmer, der er indeholdt i udsendelsen, lider tab på grund af anvendelsen af ulovligt udstyr, så er dette tab indirekte i forhold til de tab, som radio- og tv-selskaberne lider. Endvidere fremhæver Europarådet, at rettighedshaverne kan sikre deres rettigheder ved i deres kontrakt med radio- og tv-selskaberne at få indført bestemmelser om, at sidstnævnte i tilfælde af piratvirksomhed er forpligtet til at anlægge sag²².

20 I begrundelsen anfører Europarådet, at henstillingens principper udelukkende gælder for den del af dekodeudstyret, der gør det muligt at dekryptere signalet. Det vil sige, at i et system, der anvender smart-kort, er det kun kortet der er omfattet, og ikke dekodeudstyret som sådan, der ikke i sig selv muliggør dekryptering af signalet.

21 Europarådet begrundet denne undtagelse med, at sanktioner kun bør pålægges fabrikanter, importører og distributører af ulovligt udstyr, og ikke de foretagender, der udfører almindeligt salgs- og reklamearbejde (reklamebureauer, aviser og tidsskrifter).

22 Selv om rettighedshaverne kan indføre sådanne bestemmelser i deres kontrakt, udelukker det ikke, at der er behov for, at rettighedshaverne særlige interesser beskyttes uafhængig af radio- og tv-selskaberne. Når de ulovlige aktiviteter ikke blot krænker radio- og tv-selskaberne men også rettighedshaverne, vil radio- og tv-selskaberne måske ikke have interesse i hurtigt at gribe ind over for disse aktiviteter. Rettighedshaverne vil ganske vist kunne anlægge sag mod radio- og tv-selskaberne for at sikre overholdelse af de kontraktlige forpligtelser, som sidstnævnte har accepteret i forbindelse med indgåelsen af kontrakten. Men dette vil blot forsinke reaktionen over for piraterne.

Endelig foreskriver henstillingen ingen strafferetlige eller administrative sanktioner i forbindelse med besiddelse til privat brug.

Henstillingen spiller en vigtig rolle i den lovgivningsbølge, der siden begyndelsen af 1990'erne har været i gang i medlemsstaterne. Ofte har den særlovgivning om retlig beskyttelse af krypterede radio- og tv-spredningstjenester, der hidtil er vedtaget, taget udgangspunkt i de principper, som henstillingen indeholder.

Der er imidlertid tale om en tekst, der ikke er bindende, og den vedtagne lovgivning er meget forskellig, bl.a. hvad angår anvendelsesområde, forbudte aktiviteter og sanktionsniveau. Endvidere har flere af Den Europæiske Unions medlemsstater endnu ikke gennemført henstillingen i deres nationale lovgivning. Dette har ført til de nuværende lovgivningsmæssige forskelle på europæisk niveau.

2. Arbejdet i WIPO

I forbindelse med de igangværende drøftelser om udkastet til protokol til Bernerkonventionen og om det nye instrument til beskyttelse af udøvende kunstnere og fremstillere af fonogrammer, foreslås det i kapitel IX om håndhævelse af rettigheder i det udkast til memorandum, som forretningsudvalget udarbejdede i april 1994²³, at undersøge muligheden for at indføre bestemmelser om misbrug af teknisk udstyr.

Det foreslås således at lade fremstilling, import og distribution af udstyr i udlejnings- og salgsøjemed med det formål at muliggøre og lette ulovlig modtagelse af et kodet program, der radio- eller tv-transmitteres eller på anden måde tilgængeliggøres for almenheden, udgøre en ophavsretlig krænkelse.

Endvidere vil indehaverne af rettigheder til et program, der er blevet dekrypteret ved hjælp af ulovligt dekoderudstyr, kunne kræve erstatning.

Forhandlingerne om denne tekst pågår fortsat, og det er endnu for tidligt at udtale sig om muligheden for at lade sådanne bestemmelser indgå i den endelige tekst. Det skal imidlertid præciseres, at anvendelsesområdet i givet fald ikke vil blive begrænset til radio- og tv-udsendelse, men vil omfatte enhver "tilgængeliggørelse for almenheden" af beskyttede værker.

23

Dokument WIPO 9099D/COP/0691D af 29. april 1994.

KAPITEL 3: LOVGIVNINGEN I MEDLEMSSTATERNE

1. Generelt

Formålet med gennemgangen af den lovgivningsmæssige situation er at vise, hvorledes medlemsstaterne har forsøgt at løse problemet med ulovlig modtagelse af en krypteret tjeneste, dvs. modtagelse uden betaling og/eller tilladelse af personer, der ikke har tjenesteudbyderens tilladelse.

Nedenfor følger en kort gennemgang af medlemsstaternes lovgivning om ulovlig modtagelse af krypterede tjenester dog med det forbehold, at den lovgivningsmæssige situation ændrer sig meget hurtigt, og at et øjebliksbillede hurtigt kan vise sig at blive uaktuelt.

2. Den lovgivningsmæssige situation i medlemsstaterne (oversigt)

Der findes ikke i øjeblikket i Unionen en ensartet og systematisk tilgang til problemerne i forbindelse med ulovlig modtagelse af krypterede tjenester. I nogle lande findes der dog en særlovgivning, mens andre lande anvender allerede eksisterende regler, og atter andre ingen retsmidler har til at sikre beskyttelse.

Det skal i den forbindelse understreges, at selv om der med "kabel og satellit"-direktivet²⁴ er sikret en harmoniseret behandling af beskyttede værker, der anvendes i radio- og tv-spredning via satellit, og af viderespredning pr. kabel i Fællesskabet, gives der ingen støtte til operatørerne i deres kamp mod ulovlig modtagelse.

Rettighedshaverne kan faktisk på visse betingelser forbyde uautoriseret retransmission af deres værker men ikke ulovlig modtagelse, da det ikke er en handling, der falder ind under ophavsretten, der normalt dækker tilgængeliggørelse men ikke modtagelse af et beskyttet værk. De nationale lovgivninger, der indeholder direktivets principper, kan derfor ikke anvendes til at bekæmpe ulovlig modtagelse af krypterede tjenester.

24

Ovennævnte direktiv 93/83/EØF.

Tabel I: Lovgivning om beskyttelse af krypterede tjenester

lovgivning	særlovgivning				generel lovgivning	
	radio- og tv-spredning	tele-kommunikation	intellektuel ejendomsret	strafferet	illoyal konkurrence	intellektuel ejendomsret
Østrig					x	
Belgien		x			x	
Danmark						
Finland		x				
Frankrig	x			x		
Tyskland					x	
Grækenland						
Irland	x					
Italien	x					
Luxembourg						
Nederlandene				x	x	
Portugal						
Spanien						x
Sverige				x		
Det Forenede Kongerige	x		x			

2.1. Anvendelse af bestemmelserne om illoyal konkurrence og om intellektuel ejendomsret

I de lande, der ikke har en særlovgivning, har man ofte anvendt anden *mere generel lovgivning*, bl.a. om *illoyal konkurrence*, der beskytter mod handelspraksis, der er i strid med hæderlig adfærd. Anvendelsen af disse principper har i visse tilfælde gjort det muligt at forbyde fremstilling, import og markedsføring (salg, udlejning, besiddelse i erhvervsmæssigt øjemed) af uautoriseret dekoderudstyr (A,B,D,NL).

Disse foranstaltninger har normalt taget udgangspunkt i det faktum, at fremstilling og markedsføring af dekoderudstyr, der ikke er godkendt af krypteringsforetagendet, unddrager dette det *vederlag*, der normalt skal erlægges for den leverede tjeneste. Den uautoriserede fabrikant modtager et vederlag for en tjeneste (modtagelse af tjenesten), som en anden har leveret.

Konkurrencen mellem krypteringsforetagender og uautoriserede fabrikanter, der er baggrunden for at anvende bestemmelserne om illoyal konkurrence, accepteres i visse tilfælde²⁵. Det kræver imidlertid, at den involverede part reelt er til stede på markedet. Hvis der ikke er tale om beskyttelse af en kommerciel interesse, vil bestemmelserne om illoyal konkurrence faktisk ikke kunne anvendes.

Endvidere vil et søgsmål baseret på reglerne om illoyal konkurrence normalt kun kunne anvendes i forbindelse med distribution og salgsfremme af uautoriseret dekoderudstyr, mens import og besiddelse ikke er omfattet. Det betyder, at det er vanskeligt at anlægge sag, før udstyret er blevet markedsført, og man vil heller ikke kunne kræve forebyggende foranstaltninger.

²⁵

Den østrigske appelret (Teleclub mod Olbort) har eksplicit anerkendt, at der ikke nødvendigvis skal foreligge egentlig konkurrence, da varerne allerede på grund af deres karakteristika er konkurrerende.

Anden generel lovgivning har imidlertid vist sig vanskelig at anvende. Det er nemlig sådan, at den industrielle ejendomsret i tilfælde af fremstilling af uautoriseret dekoderudstyr allerede giver rettighedshaverne en vis beskyttelse. Flere dele i udstyret vil således været dækket af industrielle og intellektuelle rettigheder.

Sagsanlæg har imidlertid ofte vist at være en ineffektiv vej. For det første skal man for at bevise, at et smart-kort er en kopi af det software, som tilhører ejeren af systemet, afsløre krypteringsalgoritmen under retssagen, hvilket vil afsløre, hvilken teknologi der er anvendt og åbne mulighed for nye kopier. For det andet er der nu og da tale om lovlige kort, der ulovligt er blevet reaktiveret efter udløbet af deres gyldighedsperiode; i det tilfælde vil en sag baseret på den industrielle ejendomsrettighed, der er knyttet til kortet, ikke føre til noget.

Ofte vil krypteringsforetagenderne slet ikke have mulighed for at anlægge sag; de kan nemlig ikke lægge sag an mod fabrikanterne af ulovligt udstyr, idet de jo ikke er indehavere af de involverede industrielle ejendomsrettigheder.

2.2. Anvendelse af særlovgivning

Særlovgivning om beskyttelse af krypterede tjenester mod ulovlig modtagelse er et forholdsvis nutidigt fænomen. Det er en følge af den teknologiske udvikling, som kommunikationssektoren blev udsat for allerede i slutningen af 1970'erne. Som følge af udbredelsen af ulovligt dekoderudstyr på markederne i de lande, hvor krypteret radio- og tv-udsendelse var mest anvendt (F, GB), blev den første lovgivning indført i 1987 (F) og 1988 (GB).

Den næste lovgivningsbølge indtraf i begyndelsen af 90'erne, efterhånden som de krypterede kanaler vandt udbredelse i Europa. Det gælder Irland, Belgien (91), Italien (92), Finland og Sverige (94). Denne anden bølge er endnu ikke stoppet, således som det fremgår af den nuværende debat i Danmark i forbindelse med fremlæggelse af et lovforslag i den henseende.

I de lande, hvor der er indført lovgivning, har det normalt været i form af en særlovgivning om det audiovisuelle område, der har taget udgangspunkt i lovgivningen om ophavsret, og som indfører strafferetlige sanktioner for visse aktiviteter i forbindelse med ulovlig modtagelse af krypterede tjenester og giver operatørerne, og i visse tilfælde andre berørte parter, ret til at kræve erstatning af de ansvarlige for disse aktiviteter.

Den eksisterende nationale lovgivning om beskyttelse af krypterede tjenester kan herefter resumeres som følger:

2.2.1 *Formålet med foranstaltningerne: beskyttelse af krypterede tjenester mod ulovlig modtagelse*

Selv om de nationale lovgivninger ikke giver en entydig definition af ulovlig modtagelse, der også karakteriseres som modtagelse af betalingsprogrammer uden at have betalt licens (B, R, GB), og som adgang til krypterede tjenester uden

krypteringsforetagendets tilladelse (S, I), har de alle samme formål, nemlig at sikre, at kun de personer, der har fået tilladelse, kan modtage tjenesten.

Der eksisterer imidlertid et skel mellem de lovgivninger, der udelukkende dækker radio- og tv-udsendelse og viderespredning pr. kabel, hvor det samme program fremføres til den brede offentlighed (I, F, B, IRL, S), og de lovgivninger, der også dækker interaktive informationstjenester via telenettet (SF, GB, NL). I det sidstnævnte tilfælde skelnes der ikke mellem tjenester, der fremføres til den brede offentlighed, og tjenester, der leveres på bestilling.

Hvis der eksisterer en retlig beskyttelse mod ulovlig modtagelse af krypterede radio- og tv-spredningstjenester, vil en sådan normalt beskytte alle radio- og tv-spredningssignaler, mens det ikke altid er tilfældet for radiotjenester. Imidlertid giver nogle lande (GB, IRL) en sådan beskyttelse afhængig af oprindelse (national eller udenlandsk) eller tjenestens spredningsmåde (via satellit eller radiokæder).

Tabel II: Beskyttede tjenester

beskyttede tjenester	radio- og tv-spredning			radio	andet	betalings-tjenester
	kabel	satellit	andet			
Østrig						
Belgien	x	x	x			x
Danmark						
Finland	x	x	x	x	x	
Frankrig	x	x	x			x
Tyskland						
Grækenland						
Irland	x					x
Italien	x	x	x	x		
Luxembourg						
Nederlandene	x	x	x	x	x	x
Portugal						
Spanien						
Sverige	x	x	x	x		x
Det Forenede Kongerige	x	Kun tjenester med oprindelse i GIB	x	x	x	x

For at beskytte tjenesteudbydere mod ulovlig modtagelse har man i de nationale lovgivninger benyttet to tilgange.

Den første tilgang består i at beskytte den krypterede tjeneste. Dette sker normalt ved at anerkende krypteringsforetagendets ejendomsret til signalet. Ulovlig modtagelse af det krypterede signal betragtes herefter som "tyveri", som ejeren, dvs. krypteringsforetagendet, har ret til at blive beskyttet mod (Det Franske Sprogsamfund i Belgien, IRL, I, GB, NL, SF). Herudover forbyder denne type lovgivning ofte viderespredning, aflytning og andre aktiviteter, der kan lette og/eller muliggøre ulovlig modtagelse af signalet.

Tabel III: Typer af aktiviteter

krypterede radio- og tv-spredningstjenester	aflytning	anvendelse	transmission	organisere/muliggøret redjemands modtagelse
Østrig				
Belgien*	x		x	x
Danmark				
Finland		x		
Frankrig		x	x	x
Tyskland				
Grækenland				
Irland	x			x
Italien	x		x	
Luxembourg				
Nederlandene		x		
Portugal				
Spanien				
Sverige				x
Det Forenede Kongerige	x	x		x

* *Kun Det Franske Sprogsamfund*

Den anden tilgang indebærer, at man direkte koncentrerer sig om at forbyde *de forberedende aktiviteter* (Det Franske Sprogsamfund i Belgien, F, S). Ulovlig modtagelse vil herefter ikke blive betragtet som en ulovlig aktivitet som sådan, men de *kommercielle aktiviteter, der fremmer ulovlig modtagelse*, vil være forbudte.

Disse forskellige tilgange har følger for beskyttelsens omfang. Normalt vil den lovgivning, ifølge hvilken ulovlig modtagelse opfattes som tyveri, forbyde alle forberedende aktiviteter, både kommercielle og private. Den lovgivning, der udelukkende er koncentreret om de forberedende aktiviteter, omfatter ikke privatpersoners adfærd.

Tabel IV: Formålet med de ulovlige dekrypteringsaktiviteter

formål	kommercielt	ikke-kommercielt
Østrig		
Belgien	x	x
Danmark		
Finland	x	x
Frankrig	x	x
Tyskland		
Grækenland		
Irland	x	x
Italien	x	
Luxembourg		
Nederlandene	x	x
Portugal		
Spanien		
Sverige	x	
Det Forenede Kongerige	x	x

De forberedende aktiviteter, der enten indgår i forbuddet mod modtagelse eller udgør selve lovgivningens genstand, kan omfatte:

- a) *Fremstilling af dekoderudstyr*, der har til formål at muliggøre modtagelse af en krypteret tjeneste uden at have betalt licens

For at sikre at privatpersoner udelukkende kan modtage programmet ved hjælp af udstyr fremstillet af krypteringsforetagendet eller for dets regning, forbyder alle medlemsstaternes lovgivning fremstilling af udstyr, der udelukkende har til formål at muliggøre modtagelse af en krypteret tjeneste uden at have betalt licens (B, F, I, S, SF, NL, GB, IRL).

- b) Indførsel af dekoderudstyr, der har til formål at muliggøre modtagelse af en krypteret tjeneste uden at have betalt licens

Med den gradvise fjernelse af grænsekontrollen, er risikoen for at ulovligt udstyr, der er fremstillet i en medlemsstat, hvor en sådan fabrikation ikke er forbudt, og som en anden medlemsstat derefter kan indføre med det formål at modtage de krypterede tjenester uden at betale licens, steget stærkt. Derfor har nogle medlemsstater i deres lovgivning (B, F, I, GB, SF, IRL) forbudt indførsel af dekoderudstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens.

- c) Distribution af dekoderudstyr, der har til formål at modtage krypterede tjenester uden at betale licens

Det alvorligste angreb på krypterede tjenester er klart markedsføring af udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens. Normalt forbyder de nationale lovgivninger distribution af udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens (B, F, I, S, GB, IRL, SF, NL).

- d) Besiddelse i erhvervmæssigt øjemed af udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens

Besiddelse i erhvervmæssigt øjemed, bl.a. med henblik på salg og/eller udlejning, er en etape i den ulovlige aktivitet, der muliggør modtagelse af en krypteret tjeneste uden at betale licens; derfor er besiddelse i erhvervmæssigt øjemed forbudt i nogle landes lovgivning (B, F, I, IRL, SF, NL), idet det muliggør modtagelse af en krypteret tjeneste uden at betale licens.

- e) Privatpersoners besiddelse af dekoderudstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens

Selv om privatpersoners besiddelse af udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens, i sig selv er en mindre alvorlig forseelse end besiddelse i erhvervmæssigt øjemed, forbyder nogle medlemsstater i deres lovgivning også privatpersoners besiddelse af ulovligt udstyr (GB, NL, B, F, IRL).

- f) Salgsfremme af udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens

I de tilfælde hvor lovgivningen har til formål at beskytte tjenesteudbyderen mod ulovlig modtagelse, er salgsfremme i forbindelse med udstyr, der har til formål at muliggøre modtagelse af krypterede tjenester uden at betale licens, endvidere forbudt i nogle medlemsstaters lovgivning (B, F, GB, IRL, NL, IRL).

Tabel V: Ulovlige aktiviteter i forbindelse med dekoderudstyr

dekoderudstyr	fremstilling	indførelse	distribution	salgsfremme	besiddelse i erhvervmæssigt øjemed	besiddelse til privat brug
Østrig						
Belgien*	x	x	x	x	x	x
Danmark						
Finland	x	x	x		x	x
Frankrig	x	x	x	x	x	x
Tyskland						
Grækenland						
Irland	x	x	x	x	x	x
Italien	x	x	x	x	x	x
Luxembourg						
Nederlandene	x		x	x	x	x
Portugal						
Spanien						
Sverige	x		x			
Det Forenede Kongerige	x	x	x	x		

* *Kun Det Flamske Sprogsamfund*

Endvidere omfatter de fleste medlemsstaters lovgivning også andre lignende aktiviteter, der alle har forbindelse med markedsføring af dekoderudstyr.

Tabel VI: Andre ulovlige aktiviteter i forbindelse med dekoderudstyr

dekoderudstyr	tilpasning	salg	udlejning	installation	vedligeholdelse	anvendelse	køb	andet
Østrig								
Belgien		x	x	x			x	
Danmark								
Finland						x		
Frankrig		x		x			x	
Tyskland								
Grækenland								
Irland				x	x			
Italien		x	x					
Luxembourg								
Nederlandene								
Portugal								
Spanien								
Sverige		x	x	x	x			
Det Forenede Kongerige		x	x					

2.2.2 Sanktioner

De nationale lovgivninger foreskriver normalt strafferetlige eller administrative sanktioner, hvis loven overtrædes, samt mulighed for civile retlige erstatningssøgsmål. Der er flere muligheder i sidstnævnte tilfælde:

En mulighed er, at der i særlovgivningen intet nævnes om erstatningskrav, hvilket normalt betyder, at de generelle bestemmelser finder anvendelse (B, F, I, NL).

En anden mulighed er, at der er en specifik henvisning til reglerne om erstatningssøgsmål (det danske lovforslag). Det hedder i lovmotiverne, at tjenesteudbydere og rettighedshaverne skal kunne kræve erstatning for tab, der skyldes de uautoriserede fabrikanter aktiviteter.

En tredje mulighed er at indføje en bestemmelse, der fastslår, at de civile retlige afhjælpningsmuligheder, som rettighedshaverne har, finder anvendelse (GB). Disse civile retlige afhjælpningsmuligheder er bl.a. muligheden for at få tildelt erstatning og retten til at kræve, at den krænkende aktivitet ophører. Endelig findes der lovgivning, der giver særlige civile retlige afhjælpningsmuligheder, og fastsætter søgsmålskompetence og de mulige søgsmål (IRL).

Table VII: Sanktioner

sanktioner	bøde	fængselsstraf	administrative bestemmelser	civilretlige bestemmelser
Østrig				
Belgien	fra 26 til 100 000 BEF (fra 0,7 til 2 650 ECU)	-	konfiskation af dekoderudstyr og fortjeneste	-
Danmark				
Finland	bøde	højest 2 år	konfiskation af det ulovlige udstyr og fortjeneste	-
Frankrig	fra 5 000 til højest 200 000 FRF (fra 772 til 30 880 ECU)	højest 2 år	konfiskation af tekniske data, udstyr og reklamemateriale samt fortjeneste	
Tyskland		-		-
Grækenland				
Irland	højest 20 000 IEP (24 554 ECU)	højest 2 år	konfiskation af det udstyr, der er anvendt i forbindelse med den ulovlige handling	særlig søgsmålsret
Italien	fra 500 000 til 6 000 000 IFL (fra 220 til 2 645 ECU)	fra 3 måneder til 3 år	-	-
Luxembourg				
Nederlandene	højest 100 000 NLG (48 670 ECU)	højest 3 år	konfiskation af udstyr og fortjeneste	-
Portugal				
Spanien				
Sverige	bøde	højest 6 måneder	konfiskation af det ulovlige udstyr og fortjeneste	-
Det Forenede Kongerige	højest 5 000 GBP (6 045 ECU)	højest 2 år	søgsmålsret baseret på ophavsretten	søgsmålsret baseret på ophavsretten

2.2.3 Forskellene i medlemsstaternes lovgivning

Det fremgår af ovenstående, at de eksisterende lovgivninger er meget forskellige. Disse forskelle viser sig især på følgende områder:

- anvendelsesområde (nationale tjenester eller tjenester fra andre medlemsstater; radio- og tv-spredningstjenester eller alle krypterede tjenester, herunder bestillingstjenester)
- beskyttelsesniveau (forbud mod besiddelse til privat brug og mod salg fremme)
- søgsmålskompetence hvad angår de civile retlige afhjælpningsmuligheder (krypteringsforetagendet eller enhver interesseret part)
- sanktionsniveau.

Disse forskelle er endnu mere markante i de tilfælde, hvor der ikke findes en særlovgivning.

Konklusion

Nogle medlemsstater har siden slutningen af 1980'erne haft en særlovgivning, der beskytter krypterede tjenester mod ulovlig modtagelse ved hjælp af uautoriseret dekoderudstyr. Andre medlemsstater anvender for at sikre samme beskyttelse bestemmelser, der allerede eksisterer i anden lovgivning (illoyal konkurrence, intellektuel ejendomsret). Endelig findes der i nogle medlemsstater på nuværende tidspunkt ikke en sådan beskyttelse.

Det følger heraf, at der i Den Europæiske Union findes store forskelle i den retlige behandling af ulovlig modtagelse af krypterede tjenester; visse aktiviteter, der er forbudt i nogle medlemsstater, kan være lovlige i andre.

Spørgsmål 1: Kommissionen udbeder sig alle former for supplerende oplysninger, der kan uddybe analysen af de nationale lovgivninger.

KAPITEL 4: HINDRINGERNE FOR DET INDRE MARKEDS FUNKTION

Kommissionen mener, at de eksisterende forskelle i medlemsstaternes lovgivning kan være en hindring for den frie udveksling af tjenesteydelser og derfor kan skade det indre markeds funktion.

Nogle af disse hindringer er uforenelige med traktatens principper, og de skal fjernes. Det gælder først og fremmest de nationale lovgivninger, i hvilke der i forbindelse med retlig beskyttelse mod ulovlig modtagelse gøres forskel afhængig af tjenestens oprindelse. Det foreskrives i disse lovgivninger, at tjenester fra andre medlemsstater kun vil være beskyttet mod ulovlig modtagelse, hvis den nationale myndighed forudgående har attesteret, at de giver dem ret til en sådan beskyttelse²⁶.

I andre medlemsstaters lovgivning udelukkes visse tjenester simpelthen fra beskyttelse på grund af den anvendte transmissionsmåde. Det gælder f.eks., når det kun er radiokædebaserede eller kabelfremførte tjenester, der er beskyttet mod ulovlig modtagelse, mens krypterede tjenester, der spredes via satellit, og som alle er udenlandske, ikke har en sådan beskyttelse²⁷. Der er her tale om en skjult diskrimination.

I de tilfælde vil en tværnational ydelse af disse tjenester, som f.eks. mellem abonnent og krypteringsforetagende, blive vanskeligere end rent nationale tjenesteydelser. De nationale vil automatisk være beskyttede, mens tjenester fra andre medlemsstater ikke vil være beskyttede eller skal opnå forudgående godkendelse for at kunne drage fordel af en sådan beskyttelse. I henhold til EF-Domstolens retspraksis er sådanne foranstaltninger ikke tilladte. Diskriminerende foranstaltninger med hensyn til tjenesteydelser er nemlig kun forenelige med EF-retten, hvis de kan henføres til en undtagelsesbestemmelse, som f.eks. traktatens artikel 56, som er begrundet i hensynet til den offentlige orden, den offentlige sikkerhed eller den offentlige sundhed²⁸. I det konkrete tilfælde kan ingen af de nævnte grunde berettige en sådan diskrimination. Kommissionen kan derfor inden for rammerne af sin kontrol med anvendelsen af fællesskabsretten bringe denne diskrimination til ophør.

Derimod har analysen af de nationale lovgivninger gjort det muligt at identificere en række hindringer for den frie bevægelighed for varer og tjenesteydelser, der kan betragtes som begrundet i almene hensyn, og som derfor er forenelige med traktatens principper. For disse hindringers vedkommende kan det vise sig nødvendigt med et initiativ for at sikre det indre markeds funktion.

1. Hindringer for den frie bevægelighed for dekoderudstyr (traktatens artikel 30 ff.)

Det hedder i traktatens artikel 30, at kvantitative indførselsrestriktioner såvel som alle foranstaltninger med tilsvarende virkning er forbudt mellem medlemsstaterne²⁹. Forbud

26 Jf. Storbritanniens lovgivning.

27 Jf. den irske lovgivning.

28 Dom "Mediawet" af 25.7.1991, sag 288/89, Sml. 1991, s. I-4007.

29 I den forbindelse mindes om, at EF-Domstolen normalt definerer kvantitative restriktioner, som forbud mod eller begrænsninger af indførsel, og foranstaltninger med tilsvarende virkning som

mod fremstilling og salg gælder uden forskel³⁰ og har restriktive virkninger for samhandelen, for så vidt som de opstiller hindringer for indførsel og salg af produkter fra andre medlemsstater.

I henhold til EF-Domstolens retspraksis er disse forbud berettigede, da de er begrundet i almene hensyn. På den ene side har de til formål at beskytte krypteringsforetagendet mod personer, der ulovligt vil kunne drage fordel af dets aktiviteter (dvs. fabrikanter og distributører af uautoriseret dekoderudstyr), og at beskytte forbrugeren mod salg af udstyr, der, fordi det er uautoriseret, ikke garanterer modtagelse af tjenesten, hvis operatøren skifter system. Et sådant formål, der skal sikre, at de økonomiske transaktioner forløber på en retfærdig og loyal måde, er blandt de almene hensyn, der ifølge Domstolen kan udgøre en hindring for frie varebevægelser. Domstolen har flere gange fastlagt, at forbrugerbeskyttelse og god handelsskik kan begrunde hindringer for frie varebevægelser³¹.

"enhver af medlemsstaternes bestemmelser for handelen, som direkte eller indirekte, øjeblikkeligt eller potentielt, kan hindre samhandelen i Fællesskabet" (Dom "Dassonville" af 11.7.1974, sag 8/74, Sml. 1974, s. 837).

EF-Domstolen opstiller imidlertid inden for denne kategori et skel. På den ene side de handelsmæssige bestemmelser, der har samme virkning som kvantitative restriktioner, og som er uforenelige med artikel 30, da de udelukkende pålægger betingelser for indførte produkter, gør salg og anvendelse af disse produkter vanskeligere eller dyrere end afsætning af nationale produkter (forskelsbehandlende foranstaltning). Ifølge Domstolen kan sådanne bestemmelser, på samme måde som kvantitative restriktioner, i det omfang de er diskriminerende, udelukkende begrundes på basis af artikel 36.

På den anden side de handelsmæssige bestemmelser, der har samme virkning på indførte og nationale produkter. Domstolen har fastsat, at selv om bestemmelserne finder lige anvendelse på indenlandske og indførte produkter (ikke-forskelsbehandlende foranstaltning), må sådanne nationale bestemmelser kun medføre hindringer for et produkt, der lovligt fremstilles og/eller sælges i en anden medlemsstat, hvis det er uomgængeligt nødvendigt (Domstolen omtaler her, ud over de almene hensyn nævnt i artikel 36, beskyttelse af den offentlige sundhed, forbruger- og miljøbeskyttelse, god handelsskik osv.) (Dom "Cassis de Dijon" af 20.02.1979, sag 120/78, Sml. 1979, s. 649; "Kommissionen mod Frankrig" af 23.2.1988, sag 216/84, Sml. 1988, s. 793).

I det tilfælde vil hindringerne for den frie bevægelighed for varer som følge af forskellige nationale lovgivninger være begrundet, hvis der er en direkte forbindelse mellem lovgivningen og den uomgængelige nødvendighed (kausalitetskriterium), og hvis bestemmelserne er passende og rimelige i forhold til situationen (proportionalitetskriterium), eller der i oprindelseslandet ikke findes en tilsvarende lovgivning, og der ikke findes alternative løsninger, der gør det muligt at nå det ønskede mål, samtidig med at der skabes færre forstyrrelser for samhandelen (substitutionskriterium).

En national lovgivning kan, selv om den anvendes uden forskelsbehandling, udgøre en foranstaltning med tilsvarende virkning, når de restriktive virkninger for samhandelen inden for Fællesskabet, uanset om foranstaltningen er begrundet i uomgængeligt nødvendige hensyn, er mere vidtrækkende end nødvendigt for at nå det ønskede resultat.

30

Disse bestemmelser fremmer ikke den nationale produktion og medfører de samme restriktioner for nationale og indførte produkter.

31

Dom "Bequelin" af 25.11.1971, sag 22/71, Sml. 1971, s. 257; "Dansk Supermarked" af 22.1.1981, sag 58/80, Sml. 1981, s. 181.

På den anden side skal disse forbud sikre, at indehaverne af de intellektuelle rettigheder, der udsendes via det krypterede signal, og indehaverne af de industrielle og intellektuelle rettigheder, der indgår i udstyret, modtager vederlag³². Sikring af retten til det lovmæssige vederlag, uanset om der er tale om vederlag til indehaverne af programrettigheder eller indehaverne af rettighederne til den teknologi, der indgår i det ulovlige udstyr, er blandt de rettigheder, der ifølge Domstolens retspraksis er den særlige genstand for industriell og intellektuel ejendomsret³³.

Disse bestemmelser overholder proportionalitetskriteriet, da de blot forbyder salg af udstyr, der er fremstillet uden forudgående godkendelse af krypteringsforetagendet, uden hensyntagen til national eller udenlandsk oprindelse; de er derfor ikke mere omfattende, end det er nødvendigt for at nå det forfulgte mål³⁴. De overholder ligeledes substitutions- og ækvivalenskriteriet, da der ikke findes alternative og mindre bindende bestemmelser, der kan sikre den ønskede beskyttelse.

Konkluderende kan det siges, at hindringer for den frie udveksling af dekoderudstyr, der fremstilles og sælges i oprindelseslandet uden krypteringsforetagendets forudgående tilladelse, kan begrundes i hensynet til forbrugerbeskyttelse, god handelsskik og industrielle og intellektuelle ejendomsrettigheder.

2. Hindringer for den frie bevægelighed for dekoderudstyr (traktatens artikel 59 ff.)

Gennemgangen af medlemsstaternes lovgivning har vist, at nogle landes lovgivning forbyder aktiviteter, der støtter fremstilling og salg af ulovligt dekoderudstyr. Det gælder de lovgivninger, der forbyder salgsfremme, installation, vedligeholdelse og udskiftning af ulovligt dekoderudstyr.

Disse aktiviteter er tjenesteydelser efter traktatens artikel 59 og 60. Selv om disse forbud anvendes uden forskel, har de ikke desto mindre restriktive virkninger for den frie udveksling af tjenesteydelser. Salgsfremme og/eller service udført af udbydere, der er etableret i andre medlemsstater, vil nemlig være forbudt.

I henhold til Domstolens retspraksis³⁵ kan disse restriktive virkninger imidlertid være begrundede. Medlemsstaternes lovgivning forfølger nemlig mål, der er begrundet i

³² Derfor henvises der i nogle medlemsstaters lovgivning til de ophavsretlige bestemmelser. Disse giver de berørte parter (normalt krypteringsforetagenderne) de samme rettigheder som rettighedshaverne til et beskyttet værk i forbindelse med en ulovlig kopi af selve værket. I begge tilfælde, vil den ulovlige kopi, uanset om der er tale om et værk eller dekoderudstyr, der muliggør modtagelse af en tjeneste, udelukke rettighedshaveren eller udbyderen, fra at modtage det lovmæssige vederlag.

³³ Dom "Deutsche Grammophon" af 8.6.1971, sag 78/70, Sml. 1971, s. 125.

³⁴ Hvad angår import og salg af udstyr, der fremstilles og sælges i oprindelseslandet med krypteringsforetagendets godkendelse, vil de omhandlede forbud derimod kunne medføre økonomiske hindringer, der ikke står i forhold til det forfulgte mål, og som derfor er uforenelige med princippet om fri bevægelighed for varer, således som fortolket af Domstolen.

³⁵ Domstolen skelner mellem restriktioner, der er forskelsbehandlende, og restriktioner, der anvendes uden forskel. Førstnævnte kan retfærdiggøres af de i artikel 56 nævnte grunde (offentlig orden, offentlig sikkerhed og offentlig sundhed). Hvad angår foranstaltninger, der medfører restriktioner, der finder anvendelse uden forskel, har Domstolen fastsat, at artikel 59 ikke blot

almene hensyn, som f.eks. forbrugerbeskyttelse³⁶ og industriel og intellektuel ejendomsret³⁷. Endvidere er disse restriktive virkninger ikke mere vidtrækkende end nødvendigt for at nå det ønskede mål, og de står derfor i et rimeligt forhold dertil³⁸.

Konkluderende kan det siges, at forbud mod salg fremme, installation, vedligeholdelse og udskiftning af dekoderudstyr, der fremstilles og sælges i oprindelseslandet uden krypteringsforetagendets forudgående tilladelse, kan begrundes i hensynet til forbrugerbeskyttelse og beskyttelse af industriel og intellektuel ejendomsret.

3. Hindringer for den frie udveksling af krypterede tjenester

Hindringer for den frie udveksling af krypterede tjenester kan endvidere skyldes en manglende retlig beskyttelse i nogle modtagerlande. Således bekræftede operatørerne i forbindelse med den af Kommissionen arrangerede høring at, en effektiv retlig beskyttelse mod ulovlig modtagelse af tjenesterne er af afgørende betydning, når de skal beslutte, om de vil distribuere en given tjeneste i et land. En manglende retlig beskyttelse gør helt klart markedsføringen vanskeligere og mere risikabel. Operatørerne får ekstraomkostninger, der ikke kun skyldes, at de er nødt til at anvende et meget sikkert system, men også fordi de er nødt til at anvende distributionssystemer for dekoderudstyret (normalt udlejning), der er særdeles dyrt.

Et sådant retligt tomrum har ligeledes restriktive virkninger for udveksling af krypterede tjenester i det indre marked, idet det er vanskeligere at distribuere tjenester i de lande, der ikke sikrer en retlig beskyttelse mod ulovlig modtagelse.

Disse restriktive virkninger er imidlertid ikke i modstrid med EF-retten; EF-Domstolen har fastslået³⁹, at hvis der ikke er foretaget en EF-harmonisering, kan medlemsstaterne frit regulere de økonomiske aktiviteter på deres område i overensstemmelse med traktatens principper. De kan således under overholdelse af proportionalitetsprincippet beslutte at forbyde eller ikke at forbyde visse aktiviteter ud fra almene hensyn.

kræver afskaffelse af enhver forskelsbehandling til skade for tjenesteyderen på grund af dennes nationalitet, men også "ophævelse af enhver restriktion - også selv om den anvendes uden forskel på indenlandske tjenesteydere og tjenesteydere fra andre medlemsstater - der kan være til hinder for eller på anden måde genere den virksomhed, som udøves af en tjenesteyder med hjemsted i en anden medlemsstat, hvor han lovligt leverer tilsvarende tjenesteydelser". (Dom "Dennemeyer" af 25.7.1991, sag 76/90, Sml. 1991, s. 4221). I henhold til Domstolen følger det heraf, at et forbud, der finder anvendelse uden forskel, ikke desto mindre kan være begrænsende for den frie udveksling af tjenesteydelser, hvis der er tale om hindringer, der ikke er begrundet i tvingende almene hensyn, og kun i det omfang disse hensyn ikke allerede tilgodeses i kraft af de bestemmelser, tjenesteyderen er undergivet i den medlemsstat, hvor han er etableret, og det ikke er muligt at opnå samme resultat med mindre vidtgående regler. Blandt de tvingende almene hensyn regner Domstolen beskyttelse af forbrugere og arbejdstagere og beskyttelse af industriel og kommerciel ejendomsret osv.

36

Dom "Kommissionen mod Frankrig" af 4.12.1986, Sml. 220/83, Sml. 1986, s. 3663.

37

Dom "Coditel" af 18.3.1980, sag 62/79, Sml. 1980, s. 881.

38

Man ville formodentlig vælge en anden løsning i forbindelse med udstyr, der fremstilles og sælges i oprindelseslandet med krypteringsforetagendets tilladelse. I det tilfælde ville disse restriktioner udgøre en hindring for de økonomiske transaktioner mellem medlemsstaterne, der ikke står i forhold til det tilstræbte mål, og som derfor er uforenelig med traktatens principper om fri udveksling af tjenesteydelser, således som fortolket af Domstolen.

39

Dom "Procureur du Roi mod Debauve" af 18.3.1980, sag 52/79, Sml. 1980, s. 833.

Konkluderende kan det siges, at hvis der ikke er foretaget en EF-harmonisering, vil de enkelte medlemsstaters regulering af deres økonomiske aktiviteter, kunne retfærdiggøre, at der opstår restriktive virkninger som følge af det retlige tomrum.

4. Konkurrenceforvridning

Forskellene i de nationale lovgivninger og manglende lovgivning i nogle medlemsstater kan endvidere medføre konkurrenceforvridning i det indre marked. En operatør, der distribuerer dekoderudstyr i en medlemsstat, hvor der findes en retlig beskyttelse, vil få konkurrencemæssige fordele (der f.eks. vil afspejle sig i operatørens muligheder for at købe programmer) i forhold til den operatør, der distribuerer sin tjeneste i en medlemsstat, hvor der ikke findes en effektiv retlig beskyttelse, idet sidstnævnte vil få ekstraomkostninger, der bl.a. skyldes nødvendigheden af at anvende et særligt sikkert distributionssystem.

Disse forskellige konkurrencebetingelser i medlemsstaterne kan få negative følger for udviklingen af krypterede tjenester i det indre marked, da operatørerne i Den Europæiske Union ikke er underkastet samme markedsforhold.

Konkluderende kan det siges, at forskelle i medlemsstaternes lovgivning kan være konkurrenceforvridende, hvilket kan vanskeliggøre udviklingen af krypterede tjenester.

Spørgsmål 2: Kommissionen ønsker at få kendskab til de berørte kredsers mening om eventuelle andre restriktioner og restriktive virkninger end de ovenfor nævnte.

KAPITEL 5: BEHOVET FOR EN EF-FORANSTALTNING OG MULIGE INITIATIVER

Ovenstående analyse har vist, at der i dag er en række hindringer for det indre markeds funktion. Nogle af disse hindringer kan vise sig at være uforenelige med EF-retten, og de skal derfor fjernes. Det gælder hindringer, der skyldes, at de nationale lovgivninger med henblik på at sikre retlig beskyttelse af krypterede tjenester opstiller skel på basis af tjenestens art (radiokæde- eller satellitbaseret) eller oprindelse.

Andre hindringer kan imidlertid begrundes i almene hensyn, som f.eks. forbrugerbeskyttelse og beskyttelse af industriel og intellektuel ejendomsret samt i proportionalitetsprincippet. Det gælder først og fremmest hindringer for den frie bevægelighed for dekoderudstyr og tjenester, som er knyttet til dette udstyr, og som følger af de forskellige nationale lovgivninger om fremstilling og salg af dekoderudstyr.

Ud fra et økonomisk synspunkt viste høringen endvidere, at de forskellige lovgivningsmæssige løsninger med de ekstraomkostninger og den manglende retssikkerhed, der følger deraf, af branchen opfattes som en alvorlig hindring for udviklingen af nye krypterede tjenester. En effektiv retlig beskyttelse mod ulovlig modtagelse er således af afgørende betydning for at få investorerne til at udvikle krypterede tjenester og distribuere dem i andre medlemsstater.

For sidstnævnte hindrings vedkommende vil det være nødvendigt at indføre et ensartet beskyttelsesniveau i alle medlemsstaterne for at fjerne de hindringer, der er konstateret, og supplere den retlige ramme for det europæiske audiovisuelle område, der er indført med direktivet om "fjernsyn uden grænser" (89/552/EØF) og "kabel og satellit"-direktivet (93/83/EØF).

Det skal i den forbindelse understreges, at en fjernelse af de hindringer for det indre markeds funktion, der skyldes forskellige nationale lovgivning om retlig beskyttelse af krypterede tjenester, kun kan nå effektivt via en harmonisering på fællesskabsniveau. Det er nemlig lidet sandsynligt, at medlemsstaterne spontant foretager en tilnærmelse af deres lovgivning om retlig beskyttelse af krypterede tjenester. Selv om det skulle være tilfældet, vil den manglende institutionelle ramme, som fællesskabsretten udgør, gøre en sådan tilnærmelse lidet effektiv, og den vil ikke kunne give industrien den retssikkerhed, som udviklingen af krypterede tjenester kræver.

Før Kommissionen træffer beslutning om en eventuel EF-foranstaltning, ønsker den at få kendskab til de berørte kredsers holdning til nedenstående muligheder.

1. Formålet med initiativet

Hovedformålet skulle være at give mediebranchen (udbydere af krypterede tjenester, programproducenter eller fabrikanter af udstyr) mulighed for fuldt ud at drage nytte af det indre markeds muligheder. Disse muligheder, med alt hvad de indebærer i forbindelse med informationssamfundet, risikerer nemlig ikke at blive udnyttet, hvis virksomhederne i Unionen ikke sikres en tilstrækkelig retlig beskyttelse.

En klar lovgivningsmæssig ramme, der gør det muligt i hele Unionen at opnå en retlig beskyttelse mod ulovlig modtagelse af tjenester, og som kan sikre fri bevægelighed for varer og tjenesteydelser, er en forudsætning for udviklingen af nye tjenester.

Da problemet med ulovlig modtagelse er globalt, bør der endvidere iværksættes et arbejde på internationalt plan, bl.a. inden for rammerne af bilaterale aftaler og i forbindelse med WTO's aktiviteter, for at få indført effektive regler på verdensplan. Det ville være utilstrækkeligt at vedtage en foranstaltning blot for det indre marked; en sådan foranstaltning skal ligeledes indeholde bestemmelser, der løser problemerne på internationalt plan og giver beskyttelse mod import fra tredjelande.

2. Overensstemmelse med Fællesskabets øvrige politik

Et lovgivningsmæssigt initiativ for at sikre retlig beskyttelse af krypterede tjenester ville endvidere være i overensstemmelse med Fællesskabets øvrige mål og politik.

- En lovgivningsmæssig ramme, der sikrer en retlig beskyttelse på unionsniveau ville bidrage til at udvikle den europæiske industri inden for krypterede tjenester og fremstilling af dekoderudstyr. Hvis der ikke eksisterer en effektiv retlig beskyttelse, risikerer ulovlig modtagelse og de deraf følgende indtægtstab at ødelægge økonomien for udbydere af krypterede tjenester og gøre udviklingen af disse tjenester meget vanskelig. Det samme vil gøre sig gældende for fabrikanterne af dekoderudstyr, der i mangel af retlig beskyttelse, ikke vil kaste sig ud i aktiviteter, der ikke er sikret mod ulovlige handlinger;
- Et lovgivningsmæssigt initiativ for at sikre det indre markeds funktion vil være i overensstemmelse med målsætningerne for Unionens politik på det audiovisuelle og kulturelle område. Et sådant initiativ vil muliggøre en bedre udnyttelse af de intellektuelle ejendomsrettigheder til de programmer, som udsendes via kanalerne, hvilket vil give øgede udnyttelsesmuligheder for den audiovisuelle produktion. De nye krypterede tjenester er af afgørende betydning for udvikling og udveksling af kunstneriske aktiviteter og for en udfoldelse af den kulturelle og sproglige mangfoldighed i Unionen; rettighedshaverne vil imidlertid tøve med at afgive deres rettigheder, hvis de krypterede tjenester ikke sikres mod ulovlig modtagelse. I en sådan situation vil krypterede tjenester, af mangel på programmer, ikke blive udviklet, og den audiovisuelle produktion vil miste muligheden for at benytte en betydelig spredningsmulighed.
- Et lovgivningsmæssigt initiativ for at sikre det indre markeds funktion vil være i overensstemmelse med målsætningen om forbrugerbeskyttelse. Hvis der ikke findes en sikker retlig ramme, vil forbrugerne ved køb af dekoderudstyr kunne tage fejl af dets oprindelse og tro, at de køber autoriseret udstyr, mens der i virkeligheden er tale om en piratdekode. Hvis operatøren i det tilfælde af sikkerhedsgrunde ændrer krypteringssystemet, vil det købte udstyr ikke kunne hjælpe forbrugeren, der vil være nødt til for egen udgift at købe en anden dekode. Samtidig vil der ikke altid være garanti på ulovligt udstyr. Hvis udstyret går i stykker, vil forbrugeren selv skulle betale reparationerne. I begge

tilfælde er de negative virkninger for forbrugeren som følge af salg af ulovligt dekoderudstyr klare. Endvidere vil de tab, der påføres tjenesteudbydere, få negative følger for deres økonomi; udviklingen af krypterede tjenester vil derfor kunne blive forsinket på grund af manglende beskyttelse, og denne situation vil være et tab for forbrugerne, der ikke længere vil kunne drage fordel af tjenesterne.

3. Valg af instrument og retsgrundlag

I lyset af den gennemførte analyse vil den beslutning, som Kommissionen skal træffe efter høring af de berørte kredse, kunne antage en af følgende to former.

Kommissionen kan foreslå et direktiv om harmonisering af medlemsstaternes lovgivning (1. mulighed). I betragtning af proportionalitets- og nærhedsprincippet vil et sådant direktivforslag kunne indføre en minimal harmonisering, der giver medlemsstaterne mulighed for frit at indføre strengere regler, samtidig med at der sikres en ensartet minimumsbeskyttelse i hele Unionen. Fordelen ved denne mulighed er, at de berørte kredse derved opnår retssikkerhed samtidig med, at medlemsstaterne får et vist spillerum hvad angår omfanget af denne beskyttelse.

En anden mulighed er, at Kommissionen udarbejder et forslag til rådsforordning (2. mulighed). Formålet vil være det samme som ovenfor, men fordelene ville være en mere effektiv harmonisering, da en forordning direkte finder anvendelse i medlemsstaterne og ikke kræver indarbejdelse i den nationale lovgivning.

Den valgte løsning kan eventuelt ledsages af et forslag til ændring af EF-rettens bestemmelser om overgang til fri omsætning af varemærkeforfalskede varer fra tredjelande⁴⁰, således at disse bestemmelser ligeledes kan anvendes på dekoderudstyr. Det skal imidlertid understreges, at en sådan ændring alene ikke vil kunne give en effektiv retsbeskyttelse i Unionen. Anvendelse af bestemmelserne om varemærkeforfalskelse er frivillig for operatørerne og de berørte virksomheder, og bestemmelserne dækker kun varer fra tredjelande i forbindelse med disses indførsel i Unionen. Samhandelen mellem medlemsstaterne reguleres af national lovgivning og EF-lovgivning. Hvad angår fremstilling og salg af ulovligt dekoderudstyr anvender medlemsstaterne imidlertid ikke på nuværende tidspunkt en ensartet tilgang, hvilket fører til forskellige løsninger og, i visse tilfælde, en manglende beskyttelse. Derfor skal en foranstaltning med henblik på at sikre kontrol med indførsel fra tredjelande nødvendigvis ledsages af et lovgivningsinitiativ, der sikrer beskyttelse mod ulovlig modtagelse i Unionen.

Da formålet er at sikre det indre markeds funktion og fri bevægelighed for varer og tjenesteydelser, er det korrekte retsgrundlag artikel 57, stk. 2, artikel 66 og 100 A⁴¹.

40 Rådets forordning (EF) Nr. 3295/94 (EFT L 341 af 30.12.1994) om foranstaltninger med henblik på at forbyde overgang til fri omsætning, udførsel, genudførsel og henførsel under en suspensionsprocedure af varemærkeforfalskede og piratkopierede varer.

41 Hvis man ønsker at ændre forordningen om forfalskelse, vil retsgrundlaget fortsat være artikel 113.

4. Anvendelsesområde

Den påtænkte harmonisering vedrører de nationale lovgivninger om retlig beskyttelse af krypterede tjenester. Hvis der eksisterer bestemmelser på området, findes de ofte i medlemsstaternes lovgivning om ophavsret, radio- og tv-spredning, i civilretten eller i forvaltningsretten. Det følger heraf, at det er uden betydning, hvor de nationale bestemmelser på området findes; det afgørende er deres formål, dvs. beskyttelse af krypterede tjenester mod ulovlig modtagelse.

En sådan harmonisering bør omfatte alle krypterede tjenester, hvor kryptering anvendes for at sikre betaling af en afgift, uden at det begrænses til radio- og tv-spredningstjenester. Kategorien vil således omfatte traditionelle krypterede radio- og tv-spredningstjenester (pr. kabel, radiokæder eller via satellit), de nye radio- og tv-spredningstjenester (digital-tv, pay-per-view, near-video-on-demand) og informations-samfundets tjenester, dvs. teleformidlede bestillingstjenester (video-on-demand, bestillingsspil, interaktiv home-shopping).

Hvis en tjeneste (radio- og tv-spredningstjeneste, bestillingstjeneste) krypteres for at begrænse modtagelsen, vil der være de samme krav til beskyttelse. Hvis derimod kun radio- og tv-spredningstjenesterne var krypterede, ville det ikke være muligt at dække de nye krypteringsanvendelser, som f.eks. interaktiv adgang til data eller tjenester uden billeder (f.eks. adgang direkte fra hjemmet til en avis via satellit) eller adgang direkte fra hjemmet til videospil via satellit eller pr. kabel.

Alle krypterede tjenester som almenheden kan få dekodere til, bør kunne få samme beskyttelse. Hvis der bliver sammenfald mellem radiofonitjenester og informations-tjenester, skal definitionen af "krypterede tjenester" kunne omfatte enhver tjeneste, der kan modtages via en tv-skærm eller en computer, dvs. lydradiofonitjenester og tv-tjenester, samt informationssamfundets øvrige interaktive tjenester, således som defineret i direktivforslaget om gennemsigtighed i lovgivningen i det indre marked, dvs. teleformidlede interaktive tjenester.

Derimod bør tjenester, hvor der anvendes kryptering af andre grunde end for at sikre betaling af licens, ikke være omfattet. Det gælder tjenester, der krypteres for at sikre fortrolighed for de transmitterede meddelelser, dvs. finansielle eller telekommunikationstjenester. Disse tjenester skal udelukkes, fordi den almene interesse, der er på spil i tilfælde af aflytning, dvs. meddelelsens integritet og fortrolighed, er helt forskellig fra beskyttelse af en tjeneste, der ydes mod vederlag. Denne forskel har imidlertid både på nationalt og internationalt niveau fundet meget forskellige lovgivningsmæssige løsninger, især hvad angår foranstaltninger og sanktioner, og som gør, at de to problemer ikke kan behandles samlet.

Beskyttelse mod varer fra tredjelande bør dække alt dekoderudstyr fra tredjelande, der gør det muligt at modtage en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet.

5. Generel arkitektur

I betragtning af proportionalitetsprincippet kunne de foreslåede foranstaltninger forbyde følgende aktiviteter:

- Fremstilling af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Salg af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Besiddelse i erhvervsmæssigt øjemed af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Privatpersoners besiddelse af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Installation, vedligeholdelse og udskiftning af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Salgsfremme af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet
- Dekryptering af krypterede udsendelser uden tilladelse fra krypteringsforetagendet.

Det bør endvidere i den foreslåede foranstaltning foreskrives, at medlemsstaterne i tilfælde af krænkelse skal indføre sanktioner, der er effektive, står i et rimeligt forhold og har en afskrækkende virkning. Kommissionen har i den henseende i meddelelsen om betydningen af sanktioner for gennemførelsen af fællesskabslovgivningen⁴² erklæret, at medlemsstaterne frit kan beslutte, hvilke sanktioner de ønsker at anvende. Der kunne eventuelt indføres en forpligtelse til at give Kommissionen meddelelse om de bestemmelser, medlemsstaterne indfører i den henseende.

Alle interesserede parter bør endvidere have mulighed for at anlægge erstatningssøgsmål.

Hvad angår bestemmelserne om beskyttelse mod fri omsætning af varer fra tredjelande skal foranstaltningen forbyde import af dekoderudstyr, der muliggør modtagelse af en krypteret tjeneste uden forudgående tilladelse fra krypteringsforetagendet.

Spørgsmål 3: Kommissionen ønsker af få oplyst, om de berørte kredse mener, der er behov for en harmonisering på fællesskabsniveau.

⁴² "Kommissionens meddelelse til Rådet og Europa-Parlamentet om betydningen af sanktioner for gennemførelsen af fællesskabslovgivningen vedrørende det indre marked", KOM(95) 162 endelig udg., af 3.5.1995.

Spørgsmål 4: Kommissionen ønsker at få kendskab til de berørte kredsers holdning til de i grønbogen foreslåede harmoniseringsforanstaltninger.

Spørgsmål 5: Kommissionen ønsker at få kendskab til de berørte kredsers holdning til indholdet i en eventuel harmoniseringsforanstaltning:

- i. anvendelsesområde:**
 - a: bør en eventuel foranstaltning begrænses til at omfatte radio- og tv-spredningstjenester eller omfatte alle krypterede tjenester for at sikre licensbetaling?**
 - b: hvis man vælger den vidtrækkende foranstaltning (krypterede tjenester for at sikre licensbetaling), er det valgte kriterium relevant, eller bør man vælge et andet kriterium til at fastsætte anvendelsesområdet? I bekræftende fald, mener De, at harmoniseringsforanstaltningen bør sikre beskyttelse mod ulovlig modtagelse af alle tjenester, uanset om de er krypterede eller ej, der anvender adgangsstyringssystemer, herunder f.eks. password?**
- ii. er det relevant, at lade privatpersoners besiddelse af ulovligt dekoderudstyr være omfattet?**
- iii. mulighed for erstatningssøgsmål?**

LISTE OVER SPØRGSMÅL

Spørgsmål 1: Kommissionen udbeder sig alle former for supplerende oplysninger, der kan uddybe analysen af de nationale lovgivninger.

Spørgsmål 2: Kommissionen ønsker at få kendskab til de berørte kredsers mening om eventuelle andre restriktioner og restriktive virkninger end de ovenfor nævnte.

Spørgsmål 3: Kommissionen ønsker at få oplyst, om de berørte kredse mener, der er behov for en harmonisering på fællesskabsniveau.

Spørgsmål 4: Kommissionen ønsker at få kendskab til de berørte kredsers holdning til de i grønbogen foreslåede harmoniseringsforanstaltninger.

Spørgsmål 5: Kommissionen ønsker at få kendskab til de berørte kredsers holdning til indholdet i en eventuel harmoniseringsforanstaltning:

- i. anvendelsesområde:
 - a: bør en eventuel foranstaltning begrænses til at omfatte radio- og tv-spredningstjenester eller omfatte alle krypterede tjenester for at sikre licensbetaling?
 - b: hvis man vælger den vidtrækkende foranstaltning (krypterede tjenester for at sikre licensbetaling), er det valgte kriterium relevant, eller bør man vælge et andet kriterium til at fastsætte anvendelsesområdet? I bekræftende fald, mener De, at harmoniseringsforanstaltningen bør sikre beskyttelse mod ulovlig modtagelse af alle tjenester, uanset om de er krypterede eller ej, der anvender adgangsstyringssystemer, herunder f.eks. password?
- ii. er det relevant, at lade privatpersoners besiddelse af ulovligt dekoderudstyr være omfattet?
- iii. mulighed for erstatningssøgsmål?