COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 06.03.1996
COM(96) 76 def.

DE RECHTSBESCHERMING VAN GEËNCRYPTEERDE DIENSTEN OP DE INTERNE MARKT

RAADPLEGING OVER DE NOODZAAK VAN EEN COMMUNAUTAIRE MAATREGEL

Groenboek van de Commissie

DE RECHTSBESCHERMING VAN GEËNCRYPTEERDE DIENSTEN OP DE INTERNE MARKT

SAMENVATTING

Doel

Door de toegenomen beschikbaarheid van frequenties en het gebruik van nieuwe technologieën konden in de afgelopen jaren nieuwe omroepdiensten worden ontwikkeld, waarbij het signaal wordt geëncrypteerd om de ontvangst daarvan te beperken tot diegenen die een vergoeding hebben betaald. Om het programma te kunnen ontvangen, moet de kijker beschikken over een decodeeruitrusting waarmee hij het beeld in zijn oorspronkelijke staat kan terugbrengen.

Deze diensten vormen een markt in volle ontwikkeling, met name door de komst van digitale technologie, waarmee de communicatiecapaciteit kan worden uitgebreid. In verband met het specialistisch karakter van deze diensten is de transnationale, vaak Europese dimensie daarbij van onmisbaar belang. Deze ontwikkeling wordt echter in gevaar gebracht door piraterij. Naast de producenten van officiële decodeeruitrustingen bestaat er namelijk een bloeiende industrie van niet-erkende fabrikanten. Deze produceren en verkopen zonder toestemming van de exploitant van de dienst uitrustingen waarmee de dienst kan worden ontvangen zonder betaling van een vergoeding. Deze illegale ontvangst leidt tot aanzienlijke verliezen voor de aanbieder van de dienst en doet indirect afbreuk aan de exploitatiemogelijkheden voor de leveranciers van programma's en de officiële fabrikanten.

Derhalve heeft de Commissie reeds in het strategisch programma voor de interne markt van 22 december 1993 (COM (93) 632) het belang benadrukt van de rechtsbescherming van geëncrypteerde diensten tegen de illegale ontvangst.

Dit belang krijgt een dringender karakter in het vooruitzicht van de informatiemaatschappij. In een toekomst waarin een veelvoud van geëncrypteerde diensten zullen worden aangeboden, moet ongeacht de inhoud daarvan worden gewaarborgd dat deze beschermd worden tegen ontvangst door diegenen die hiervoor geen toestemming hebben.

Hiertoe heeft de Commissie in haar Mededeling "Europa op weg naar de informatiemaatschappij : een actieplan" uit juli 1994 (COM (94) 347) de voorbereiding van een "Groenboek betreffende de rechtsbescherming van geëncrypteerde diensten op de interne markt" aangekondigd om de problemen te analyseren die het gevolg zijn van het ontbreken van specifieke wetgeving inzake de rechtsbescherming van geëncrypteerde diensten in bepaalde Lid-Staten en van de verschillen tussen de bestaande wettelijke regelingen in de overige Lid-Staten.

De situatie met betrekking tot de wetgeving

Uit een vergelijkende analyse van de benaderingen die door de wetgevers van de Lid-Staten zijn gevolgd, blijkt dat de oplossingen die voor het probleem van de illegale ontvangst zijn gekozen aanzienlijk uiteenlopen.

Sommige Lid-Staten hebben sinds het einde van de jaren tachtig *specifieke wetgeving* vastgesteld voor de bescherming tegen de illegale ontvangst van geëncrypteerde diensten, bepaalde andere Lid-Staten (A, P, E, GR, DK, D, LUX) nog niet.

Algemene wetgeving die soms door deze laatste Lid-Staten wordt toegepast (bij voorbeeld die op het gebied van oneerlijke concurrentie, telecommunicatie of auteursrecht) biedt vaak geen doelmatige bescherming tegen de illegale ontvangst van geëncrypteerde diensten. Hierdoor heeft zich in bepaalde van deze Lid-Staten een levendige clandestiene industrie kunnen ontwikkelen, die illegale apparatuur produceert, verkoopt, installeert en onderhoudt. Bovendien heeft zich een gespecialiseerde pers ontwikkeld met gerichte publikaties en commerciële reclame voor illegale apparatuur. De gevolgen van deze situatie doen zich ook in andere Lid-Staten gevoelen waar deze uitrustingen ondanks restrictieve maatregelen op de markt verschijnen.

Wat de Lid-Staten betreft die over specifieke wetgeving beschikken, zijn de *verschillen tussen de gekozen oplossingen* aanzienlijk, met name met betrekking tot het toepassingsgebied, de verboden activiteiten (reclame, bezit door particulieren) en de strafmaat.

Noodzaak van een communautaire maatregel

In deze situatie *kan een communautaire maatregel gerechtvaardigd zijn*. Het ontbreken van een gelijkwaardig beschermingsniveau in alle Lid-Staten heeft een *verstoorde werking van de interne markt* tot gevolg. Het leidt tot bepaalde belemmeringen voor het vrije verkeer van geëncrypteerde diensten en decodeeruitrustingen en in zeer veel opzichten tot een ongelijke concurrentiesituatie voor marktdeelnemers in verschillende Lid-Staten. De huidige *gefragmenteerde regelgeving*, welke gepaard gaat met extra economische kosten en rechtsonzekerheid, wordt door de betrokken kringen ervaren als een *belangrijk obstakel voor de ontwikkeling van een Europese markt van nieuwe geëncrypteerde diensten*.

Een dergelijk wetgevingsinitiatief zou ook nuttig zijn in het licht van de komst van de *informatiemaatschappij*, waarin geëncrypteerde diensten mogelijk een belangrijke rol gaan spelen. Een communautaire maatregel zou tevens het voordeel hebben dat de versplintering binnen de interne markt daarmee wordt weggenomen en dat tegelijkertijd rekening kan worden gehouden met andere communautaire doelstellingen als die van *het industriebeleid, het audiovisueel beleid, het cultuurbeleid en de bescherming van de consumenten*.

De marktdeelnemers hebben zich in grote meerderheid voorstander verklaard van een communautair initiatief. In dit verband heeft de *Digital Video Broadcasting Group (DVB)* een aanbeveling vastgesteld, waarin de noodzaak van een helder en uniform regelgevingskader op het niveau van de Unie wordt onderstreept. Dit verlangen wordt overigens gedeeld door het *Europees Parlement*, dat heeft voorgesteld om in de richtlijn inzake het gebruik van normen voor het uitzenden van televisiesignalen een considerans op te nemen over de noodzaak van de totstandbrenging en toepassing van doelmatige anti-piraterijwetgeving op Europees niveau. Deze considerans is door de *Raad* overgenomen tijdens de vaststelling van de richtlijn op 24 oktober 1995.

Alvorens een maatregel voor te stellen, zou de Commissie evenwel de opvatting van de belanghebbende partijen over de in het navolgende uiteengezette maatregel willen vernemen.

De Commissie zou een *initiatief tot harmonisatie van de nationale wetgeving* kunnen voorstellen. Rekening houdend met de beginselen van proportionaliteit en subsidiariteit, zou daarbij een minimum-harmonisatie kunnen worden voorgeschreven, waarbij de Lid-Staten vrij zouden zijn om striktere beginselen te hanteren, maar een *gelijkwaardig minimum-beschermingsniveau* binnen de Unie zou worden gewaarborgd. Het initiatief zou een verbod kunnen behelzen op de vervaardiging, de verkoop, het bezit voor commerciële en privatieve doeleinden, de installatie van en de reclame voor decodeeruitrustingen die bestemd zijn de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisaties. Deze maatregel zou het voordeel hebben dat een gelijkwaardige bescherming wordt gewaarborgd op het niveau van de Europese Unie tegen de illegale ontvangst van geëncrypteerde diensten en dat rechtszekerheid wordt geboden aan de betrokken kringen.

Volgende fase

De Commissie streeft naar een *open raadpleging* over het groenboek : elk persoon en elke onderneming, organisatie of autoriteit kan reageren. Het betreft hier een dubbele raadpleging, hetgeen wil zeggen dat deze niet uitsluitend gericht is tot federaties of beroepsorganisaties, maar ook tot alle individuele marktdeelnemers. Dit groenboek zal worden toegezonden aan het Europees Parlement, het Economisch en Sociaal Comité, het Comité van de Regio's, de Lid-Staten, de Europese Economische Ruimte en de landen van Midden- en Oost-Europa.

De termijn voor het indienen van de bijdragen is 31 mei 1996. Op basis van de ontvangen bijdragen zal de Commissie in de zomer van 1996 een beslissing nemen over de noodzaak van een initiatief op communautair niveau.

INLEIDING

I. Het probleem van de illegale ontvangst

Op omroepgebied wordt de laatste jaren steeds vaker gebruik gemaakt van de *encryptie van signalen*. Sinds de jaren tachtig is een aantal systemen ontwikkeld waarbij, met uiteenlopende veiligheidsniveaus, een vorm van encryptie wordt toegepast om het oorspronkelijke beeld en/of geluid voorafgaand aan de uitzending zodanig te vervormen, dat een gewone ontvanger de uitzending niet in zijn oorspronkelijke staat kan terugbrengen. Hiervoor heeft de kijker een *specifieke decodeeruitrusting* nodig (decoder, *smart card* of computerprogramma), die in staat is om de met het geëncrypteerde signaal meegezonden instructies te begrijpen. Deze uitrustingen worden doorgaans tegen betaling van een vergoeding geleverd.

Deze technologie werd oorspronkelijk gebruikt door de kabelmaatschappijen om het aantal voor de kijker beschikbare kanalen af te stemmen op de omvang van diens abonnement, en heeft zich snel uitgebreid tot betaaltelevisiezenders op de grond. Vervolgens maakte deze technologie een sterke ontwikkeling door bij de uitzending van geëncrypteerde programma's per satelliet. Het gebruik van encryptie zal evenwel explosief toenemen met de invoering van digitale technologie en met de ontwikkeling van diensten in de informatiemaatschappij als *interactief telewinkelen, informatiediensten op afstand, professionele on-line diensten, interactieve spelletjes, enzovoorts, waarbij in wisselende mate gebruik zal worden gemaakt van encryptie om de ontwikkeling daarvan commercieel levensvatbaar te maken.*

Voor het gebruik van encryptie kunnen verschillende redenen bestaan. Naast de *commercieel-strategische redenen*, die voortvloeien uit de noodzaak *nieuwe inkomstenbronnen* te vinden, is het ook nodig dat de houders van auteursrechten de *bescherming en exploitatie van de via het signaal uitgezonden programma's* zeker stellen. Ook de *bescherming van minderjarigen* kan in dit verband een belangrijke rol spelen, vooral bij kanalen voor volwassenen, evenals de mogelijkheid om de markt beter te identificeren voor "gerichtere" *reclame*.

Naast de fabrikanten van erkende decodeeruitrustingen heeft zich echter een bloeiende industrie van *niet-erkende fabrikanten* ontwikkeld. Deze clandestiene industrie vervaardigt en verkoopt decodeeruitrustingen die de *ontvangst van de dienst zonder toestemming van de dienstverrichter* mogelijk maken, doorgaans tegen een lagere prijs dan die van de erkende uitrustingen.

Geschat wordt dat deze illegale uitrustingen momenteel tussen *5 en 20 %* van alle in omloop zijnde uitrustingen vertegenwoordigen en dat zij jaarlijks tot miljoenen ecu's aan omzetverlies leiden. Deze illegale markt heeft overigens geleid tot een *gespecialiseerde pers*, met gerichte publikaties en reclamekanalen voor illegale apparatuur. Daarnaast wordt ook service na de verkoop geboden, waarbij onderhoud wordt verricht en de uitrustingen soms zelfs vervangen worden, wanneer de exploitant van systeem is veranderd.

De verkoop van deze illegale uitrustingen heeft in de eerste plaats negatieve gevolgen voor de activiteiten van *exploitanten van geëncrypteerde diensten*. Naast de verliezen die

zij ondervinden (aan potentieel marktaandeel en in de vorm van gederfde winsten), zien zij zich tevens gesteld tegenover extra kosten, omdat zij zeer dure distributiesystemen voor de decodeeruitrustingen moeten invoeren (meestal verhuur) om toezicht uit te kunnen oefenen op het gebruik van deze uitrustingen.

Ook voor de *leveranciers van de uitgezonden programma's* leidt de verkoop van illegale uitrustingen tot winstderving, omdat de particulieren die de programma's met behulp van een illegale uitrusting ontvangen niet in aanmerking worden genomen bij de onerhandelingen over de vergoeding voor de overdracht van rechten, waarbij onder meer rekening kan worden gehouden met het aantal op de dienst geabonneerde personen.

Bovendien doet de verkoop van illegale uitrustingen voor de *leveranciers van de technologie* afbreuk aan het vertrouwen van de markt in hun systeem, en leidt deze tot verliezen die verband houden met de potentiële markt die door deze uitrustingen bediend wordt.

Tenslotte betekent de verkoop van illegale uitrustingen een risiko voor de consumenten, die op het moment van aankoop misleid zouden kunnen worden omtrent de herkomst van de decoder en geloven een geautoriseerd apparaat te hebben gekocht, terwijl het in werkelijkheid om een piratendecoder gaat. Als de dienstverrichter in zo'n geval om beveiligingsredenen de versleuteling wijzigt, zal het gekochte apparaat onbruikbaar worden voor de consument, die dan op eigen kosten een andere decoder zal moeten kopen. Bovendien verrekenen de dienstverrichters de verliezen die zij lijden ten gevolge van piraterij in de verkoops- of huurprijs van de door de consument rechtmatig verworven apparatuur.

II. De situatie met betrekking tot de wetgeving

Om aan deze situatie een einde te maken, hebben de marktdeelnemers aangedrongen op de vaststelling door de Lid-Staten van specifieke regelgeving die een *snelle en efficiënte rechtsbescherming biedt* tegen de vervaardiging en distributie van illegale decodeeruitrustingen. Weliswaar heeft de *technologische vooruitgang* geleid tot een hoger veiligheidsniveau van encryptiesystemen, maar uitsluitend technologische oplossingen zijn vaak ondoelmatig gebleken. Bij de keuze van een encryptiesysteem zal de marktdeelnemer rekening houden met de kosten van dat systeem, en een hoog veiligheidsniveau dat tegelijkertijd zeer duur is kan economisch onhaalbaar blijken. Anderzijds is uit ervaring gebleken dat de ontwikkeling van illegale technieken gelijke tred houdt met de ontwikkeling van de encryptietechnieken, en dat zelfs bij gebruik van digitale technologie inbreuken op de nieuwe systemen niet kunnen worden uitgesloten. Om het hoofd te bieden aan deze illegale industrie is het nodig gebleken nieuwe regels vast te stellen die de technologische aanpak aanvullen. Dit heeft geleid tot *wetgevingsactiviteiten op het niveau van de Lid-Staten*, die nog voortduren en waarbij sterk uiteenlopende benaderingen zijn gevolgd[1].

In dit verband heeft de Commissie in haar Mededeling "Europa op weg naar de informatiemaatschappij : een actieplan" (COM(94) 347) van juli 1994 de voorbereiding van een *Groenboek inzake de rechtsbescherming van geëncrypteerde diensten op de*

[1] Zie Hoofdstuk 3 : De wetgeving van de Lid-Staten.

interne markt" aangekondigd om de problemen te analyseren die voortvloeien uit het ontbreken van specifieke regelgeving met betrekking tot de illegale ontvangst van geëncrypteerde diensten in bepaalde Lid-Staten en uit de verschillen tussen de bestaande regelingen in de overige Lid-Staten.

III. De relevante diensten

De volgende analyse heeft derhalve betrekking op de *illegale ontvangst van een geëncrypteerde dienst*, dat wil zeggen, de ontvangst zonder betaling en/of goedkeuring, door personen die niet zijn erkend door de verrichter van de diensten, alsmede op de oplossingen die in de nationale regelingen voor dit probleem zijn gevonden. Onder *geëncrypteerde diensten* moeten diensten worden verstaan waarbij gebruik is gemaakt van *encryptie van het signaal om de betaling van een vergoeding zeker te stellen*. Deze categorie omvat derhalve de *traditionele geëncrypteerde omroepdiensten* (via de kabel, de ether of per satelliet), de *nieuwe omroepdiensten* (digitale televisie, *pay-per-view*, *near-video-on-demand*) en de *diensten van de informatiemaatschappij*, dat wil zeggen, de diensten die elektronisch op afstand worden geleverd op individuele aanvraag van degene tot wie de dienst gericht is (met name video op aanvraag, spelletjes op aanvraag, elektronische verkoop, multimediadiensten).

De analyse heeft evenwel geen betrekking op diensten die worden geëncrypteerd om andere redenen dan het zeker stellen van de betaling van een vergoeding, zoals bijvoorbeeld het waarborgen van de *integriteit en de vertrouwelijkheid van de verzonden boodschap* bij financiële diensten of telecommunicatiediensten (met name mobiele-telefoondiensten waarbij GSM-technologie wordt gebruikt). Deze diensten zijn uitgesloten, omdat het *algemeen belang* dat bij onderschepping in gevaar wordt gebracht, te weten de integriteit en de vertrouwelijkheid van de communicatie, sterk verschilt van de bescherming van de waarde van een dienst die tegen betaling verricht wordt als doelstelling van algemeen belang die bedreigd wordt door de illegale ontvangst. Dit verschil heeft op nationaal en internationaal niveau geleid tot *wetgevingsoplossingen die sterk uiteenlopen*, met name wat betreft de maatregelen en de strafmaat, waardoor een gemeenschappelijke behandeling van de beide problemen niet gerechtvaardigd is.

Het groenboek heeft evenmin betrekking op vraagstukken die verband houden met systemen die het *maken van kopieën* van werken of andere beschermde bijdragen verhinderen. Deze zijn reeds behandeld in het groenboek over het auteursrecht in de informatiemaatschappij, die de Commissie in juli 1995 heeft vastgesteld.

Ten slotte wordt in het groenboek ook voorbijgegaan aan vraagstukken die verband houden met de *standaardisering van systemen voor voorwaardelijke toegang*, aan de voorwaarden voor de verlening van licenties voor deze systemen, welke reeds bestreken worden door de richtlijn inzake het gebruik van normen voor het uitzonden van televisiesignalen[2] en aan de vraagstukken in verband met de *controle door de nationale autoriteiten* op codeersystemen. Met betrekking tot laatstgenoemde vraagstukken, die nauw verbonden zijn met het probleem van de *veiligheid*, verricht de Comissie momenteel werkzaamheden in het kader van haar beleid op het gebied van de veiligheid

---

[2] Richtlijn 95/47 van het Europees Parlement en de Raad van 24 oktober 1995 inzake het gebruik van normen voor het uitzenden van televisiesignalen (PB nr. L 281/51 van 23.11.1995).

van informatiesystemen. Overigens kunnen aparte maatregelen worden genomen, indien de goede werking van de interne markt bedreigd zou worden door de toepassing van nationale rechtsregels.

IV. De voorbereidende werkzaamheden

Met het oog op de voorbereiding van het groenboek heeft de Commissie drie onafhankelijke bedrijven verzocht studies uit te voeren inzake de technologische, economische en juridische aspecten van de markt voor geëncrypteerde diensten[3].

De eerste studie (*"Technical aspects related to encrypted broadcasts"*) heeft voornamelijk betrekking op de economische en technische aspecten van het onderwerp en behandelt met name de momenteel gebruikte encryptiesystemen, de voor- en nadelen en de kwetsbaarheid daarvan. In economisch opzicht richt de studie zich op de beheerskosten van een encryptiesysteem met abonnees, op de ontwikkeling naar compatibele systemen en op de komst van nieuwe digitale technologieën.

De tweede studie (*"Protection of encrypted broadcasts"*) gaat over de juridische aspecten. Hierin wordt een analyse gemaakt van de factoren die de ontwikkeling van geëncrypteerde omroepdiensten hebben bepaald, de oorzaken van het illegale circuit en de juridische oplossingen die zijn gekozen om dit circuit het hoofd te bieden.

De derde studie (*"Legal protection of encrypted broadcasting signals"*) bevat een analyse van de bestaande wetgeving in de Lid-Staten op het gebied van de bescherming van geëncrypteerde signalen en van de tenuitvoerlegging daarvan door de nationale rechter, alsmede van de eventuele controlemechanismen en sancties. Tevens wordt een analyse gemaakt van de door internationale instanties (Raad van Europa, WIPO) vastgestelde regels.

In maart 1995 heeft de Commissie bovendien een *grootschalige raadpleging* georganiseerd van de industriesectoren welke betrokken zijn bij het probleem van de illegale ontvangst van geëncrypteerde diensten, zoals met name omroepbedrijven, fabrikanten van decodeerapparatuur, kabelmaatschappijen, leveranciers van programma's, telecommunicatiebedrijven, maar ook elke andere partij die aan de raadpleging wenste deel te nemen.

De uitkomsten van deze raadpleging hebben bevestigd dat de *illegale ontvangst van geëncrypteerde diensten* en *het gefragmenteerde karakter van het regelgevingskader op unieniveau* wezenlijke problemen vormen voor de media-industrie. Wanneer besloten moet worden of een nieuwe geëncrypteerde dienst al dan niet in een Lid-Staat

---

[3] Deze studies kunnen op verzoek bij de Commissie worden opgevraagd op onderstaand adres :
Europese Commissie, Directoraat-generaal Interne markt en financiële diensten,
Media, publiciteit en oneerlijke concurrentie,
DG XV/E/5 C107 8/59
Wetstraat 200
1049 Brussel
België
Fax : +32.2.295.77.12
E-mail : e5@dg15.cec.be

gedistribueerd zal worden, speelt de mogelijkheid om een adequate rechtsbescherming te kunnen genieten tegen illegale ontvangst voor deze industrie een belangrijke rol. *Wanneer een dergelijke rechtsbescherming ontbreekt, kiezen de marktdeelnemers er vaak voor deze dienst niet op de markt te brengen*.

De marktdeelnemers hebben zich derhalve in grote meerderheid voorstander verklaard van een communautair initiatief. In dit opzicht heeft de *Digital Video Broadcasting Group (DVB)*, dat aan de basis stond van de standaardisering van normen voor digitale televisie[4], in het kader van haar werkgroep inzake piraterij van geëncrypteerde diensten, in 1995 een aanbeveling vastgesteld, waarin de noodzaak wordt onderstreept van een helder en uniform regelgevingskader op het niveau van de Unie, waarop vertrouwd kan worden in het geval van illegale ontvangst van geëncrypteerde diensten.

Dit verlangen wordt overigens gedeeld door het Europees Parlement, dat in het kader van de procedure tot vaststelling van de richtlijn inzake het gebruik van normen voor het uitzenden van televisiesignalen heeft voorgesteld om in die richtlijn een considerans op te nemen, waarin benadrukt wordt dat de mogelijkheden voor piraterij toenemen met de digitale technologie in de Europese audiovisuele industrie, en dat de noodzaak van de vaststelling en toepassing van doelmatige anti-piraterijwetgeving op Europees niveau voortdurend toeneemt. Deze considerans is door de *Raad* overgenomen tijdens de vaststelling van de richtlijn op 24 oktober 1995.

4 Genoemde Richtlijn 95/47.

Hoofdstuk 1 : De ontwikkeling van de Europese markt van geëncrypteerde diensten

1. Een markt in volle ontwikkeling

De *technologische ontwikkelingen* (zoals het gebruik van satellieten en glasvezelkabel) hebben de laatste jaren geleid tot een ingrijpende wijziging van het audiovisuele landschap in Europa en een voortdurende uitbreiding van aangeboden diensten mogelijk gemaakt. Aangezien een groeiend aantal aanbieders gebruik maakt van *gerichte commerciële strategieën*, is encryptie van het signaal noodzakelijk gebleken om commercieel haalbare diensten te kunnen verrichten.

De traditionele structuur van de financiering van particuliere zenders, die uitsluitend was gebaseerd op inkomsten uit reclame, is voor nieuwe marktdeelnemers vaak niet toereikend. Met de groei van het aantal zenders neemt de bijdrage per zender van de traditionele reclamemakers af. Tegelijkertijd streven de marktdeelnemers ernaar zich te onderscheiden van het groeiende aantal potentiële concurrenten door in te spelen op de specifieke vraag van *nichemarkten*, die afhangt van de smaak en de belangstelling van degene tot wie de zender zich richt (filmzenders, muziekzenders, sportzenders, enzovoorts). Zo profileert de marktdeelnemer zich ten opzichte van zijn concurrenten op de massamarkt door zich te richten op deze specifieke vraag, die voorheen nauwelijks of niet onderkend was. In eenzelfde geografisch gebied is het publiek van een nichedienst echter noodzakelijkerwijze specifieker en derhalve kleiner. De exploitanten van gerichte media kunnen daarom niet rekenen op de inkomsten die de reclamemakers[5] van de massamarkt opleveren, omdat deze minder geïnteresseerd zijn in een strategie die niet op het grote publiek is gericht.

1.1. Redenen voor het gebruik van encryptie

De voornaamste redenen voor encryptie van het signaal kunnen als volgt worden samengevat :

- *De noodzaak om de financiële bijdrage door de ontvangers van de dienst zeker te stellen :* de opzet van een gerichte dienst is gebaseerd op de mogelijkheid ten opzichte van de voor het grote publiek bestemde diensten een toegevoegde waarde te bieden aan een bepaalde doelgroep. Van de ontvangers van de dienst kan derhalve een bijdrage in de financiering van de dienst worden verlangd, en dankzij encryptie kunnen de niet-abonnees van ontvangst worden uitgesloten.

- *De mogelijkheid om de reclame-opbrengsten per publiekseenheid te vergroten :* door encryptie van het signaal kan de exploitant zijn reclamezendtijd beter verkopen of zijn programma's gemakkelijker laten sponsoren door ondernemingen die belang hebben bij deze nichemarkten. In dit geval betaalt de

---

5 In dit document wordt de term "reclamemakers" gebruikt voor de "ondernemingen die gebruik maken van reclameboodschappen". Deze term omvat alle vormen van reclame, verkoopbevordering, direct marketing, sponsoring en public relations. De voorkeur wordt gegeven aan de bredere betekenis, om rekening te kunnen houden met de recente en toekomstige ontwikkelingen in het gebruik van marketinginstrumenten die het gevolg zijn van de ontwikkelingen op mediagebied.

reclamemaker niet meer voor een gehele geografische markt, maar uitsluitend voor de doelgroep. Hierbij is hij bereid een hogere prijs per publiekseenheid te betalen, omdat de kwaliteit daarvan hoger wordt ingeschat dan die van het publiek van de massamedia.

- *De mogelijkheid van een gerichter aanbod:* Door een betere kennis van de ontvanger van de dienst kan de exploitant zijn dienst aanpassen aan de specifieke vraag van de doelgroep.

- *De vereenvoudigde verwerving van uitzendrechten:* De uitzending per satelliet heeft het potentiële ontvangstbereik zeer aanzienlijk uitgebreid. Traditioneel worden uitzendrechten echter verleend op territoriale basis, waardoor het noodzakelijk is de ontvangst te beperken tot kijkers binnen een bepaald geografisch of taalgebied. Door encryptie kan de exploitant de ontvangst van het signaal beperken tot de gebieden waarvoor rechten zijn verworven. Bovendien kan door encryptie, zoals vastgesteld is in de richtlijn "kabel en satelliet"[6], bij de verwerving van uitzendrechten voor satelliet en kabel rekening worden gehouden met het werkelijke publiek (bijvoorbeeld het aantal abonnees, en niet het geografisch bereik), waardoor de aankoop van programma's voor een nichedienst minder duur is.

- *Een extra uitzendmoment wordt gecreëerd:* De geëncrypteerde uitzending van een programma biedt de houders van de rechten een extra uitzendmoment, omdat de aanbieders van een geëncrypteerde dienst vaak werken uitzenden voordat deze voor het grote publiek worden uitgezonden, en zij doorgaans bereid zijn om voor dit exclusieve recht hoge bedragen te betalen. De houders van de rechten ontvangen aldus extra inkomsten.

- *Wettelijke vereisten:* Om maatschappelijke redenen, met name de *bescherming van minderjarigen*, (bijvoorbeeld in het geval van kanalen die zich tot een volwassen publiek richten), kunnen de autoriteiten, zoals bepaald is in de richtlijn Televisie zonder grenzen[7] (artikel 22, tweede volzin), toestemming voor deze diensten geven op voorwaarde dat zij geëncrypteerd worden om de ontvangst te beperken tot bepaalde categorieën kijkers.

1.2. De geëncrypteerde diensten

De Europese markt van geëncrypteerde diensten bestaat momenteel voornamelijk uit *betaaltelevisiekanalen*[8]. Deze diensten werden aanvankelijk aangeboden per kabel en via

---

6 Richtlijn 93/83 van de Raad van 27 september 1993 tot coördinatie van bepaalde voorschriften betreffende het auteursrecht en naburige rechten op het gebied van de satellietomroep en dedoorgifte via de kabel (PB nr. L 248/15 van 6.10.1993).

7 Richtlijn 89/552 van de Raad van 3 oktober 1989 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de Lid-Staten inzake de uitoefening van televisie-omroepactiviteiten (PB nr. L 298/23 van 17.10.1989).

8 De term "betaaltelevisie" wordt hier gebruikt voor de situatie waarin de kijker betaalt om een bepaalde zender via de ether, satelliet en/of kabel te kunnen ontvangen.

de ether, en namen een vlucht toen de rechtstreekse ontvangst van telecommunicatiesatellieten met een middelgroot en groot vermogen mogelijk werd, waarbij een uitzending overal binnen het bereik van de satelliet kan worden ontvangen met een schotelantenne.

De ontwikkeling van de technologie heeft de introductie van meer geavanceerde betaaltelevisiediensten mogelijk gemaakt, zoals *pay-per-view* diensten[9], waarbij de kijker betaalt om bepaalde programma's te kunnen ontvangen. Hoewel deze diensten zelfs technisch mogelijk zijn zonder digitale compressie, is voor *pay-per-view* een geavanceerd systeem nodig voor het beheer van de abonnementen. Bij *pay-per-view* kan de kijker immers betalen voor een afzonderlijk evenement (bijvoorbeeld een concert of een bokswedstrijd) of voor een serie evenementen (bijvoorbeeld het recht om tien voetbalwedstrijden te zien). In dit laatste geval kan de zender momenteel nog niet nagaan welke evenementen de kijker heeft gezien. Er worden evenwel systemen ontwikkeld waarbij de houders van de rechten in de toekomst betaald kunnen worden voor de werkelijke "consumptie" van hun programma's.

De volgende fase is waarschijnlijk *near-video-on-demand*, waarbij het kanaal voortdurend hetzelfde programma (meestal een film, maar niet altijd) uitzendt op verschillende tijdstippen. De kijker kan dan niet alleen het programma, maar (binnnen bepaalde grenzen) ook het tijdstip kiezen. Deze dienst zal worden gevolgd door een werkelijke *video-op-aanvraag*-dienst, waarbij de kijker een grotere vrijheid heeft om het moment te kiezen waarop de film begint. Dit moment wordt dan niet langer vooraf door de zender bepaald.

De explosieve groei van het gebruik van encryptie zal gepaard gaan met de ontwikkeling van andere diensten van de informatiemaatschappij : niet slechts diensten binnen de traditionele audiovisuele sector, maar ook allerlei andere toepassingen, zoals *interactief telewinkelen, informatiediensten op afstand, professionele "on-line" diensten en interactieve spelletjes* zullen in verschillende mate geëncrypteerd worden om de ontwikkeling daarvan commercieel rendabel te maken. Aangezien encryptie bovendien vaak essentieel is met het oog op de veiligheid (zoals bijvoorbeeld van de elektronische betaling bij telewinkelen), maakt de synergie tussen deze beide toepassingen (het abonnementsysteem vergroot de veiligheid) het gebruik van encryptie - mits rechtszekerheid wordt geboden - nog geschikter om de ontwikkeling van alle diensten in de informatiemaatschappij te bevorderen.

De ontwikkeling van deze nieuwe diensten zal echter in grote mate afhangen van de totstandbrenging van een wettelijk kader waarbij rekening wordt gehouden met de legitieme verlangens van zowel de exploitanten als de ontvangers van de diensten. In dit opzicht zijn de oplossingen die op wereldschaal worden gekozen voor de diverse veiligheidsproblemen die elektronische transacties met zich meebrengen van groot belang, met name op het punt van de wettelijke beperkingen op het gebruik van encryptie, de controle op geëncrypteerde boodschappen door de autoriteiten om redenen van nationale veiligheid en de vaststelling en verificatie van de identiteit van de partijen.

---

[9] In de Verenigde Staten is 35 % van de kabelhuishoudens (ongeveer 20.000.000) uitgerust met een uitrusting voor de ontvangst van deze diensten. In Frankrijk biedt Multivision twee *pay-per-view* kanalen aan aan 220.000 huishoudens.

In dit verband onderzoekt de Commissie in het kader van haar activiteiten op het gebied van de veiligheid van informatiesystemen de mogelijkheid om op Europees niveau organen in te stellen die, volledig onafhankelijk van de overheid, belast zouden zijn met controle en certificering.

2. Een Europese markt

Momenteel telt Europa 180 televisiekanalen die via 27 satellieten worden uitgezonden[10], en bij een aanzienlijk deel daarvan (79) wordt gebruik gemaakt van min of meer geavanceerde vormen van encryptie (Tabel 1). Veel van deze kanalen zijn meer thematisch dan algemeen (bijvoorbeeld kinderprogramma's, sportzenders, filmzenders, enzovoorts).

Tabel 1 : Aantal abonnees van de belangrijkste betaaltelevisiezenders (x 1000)[11]

	A	B	CH	D	DK	E	Eir	F	Fin	I	L	NL	P	S	VK
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			
Totaal	35	302	90	855	145	903	0	142	8	655	0	162	0	612	5814

Voor de toekomst kan een sterke uitbreiding van het aanbod van geëncrypteerde diensten op Europees niveau worden verwacht. Door de lancering van nieuwe, volledig digitale satellieten (zoals Astra 1e en 1f) en de uitbreiding van de glasvezelnetten kunnen de reeds aanwezige marktdeelnemers hun aanbod uitbreiden. In dit opzicht hebben diverse exploitanten reeds in de pers hun voornemens tot introductie van digitale zenderpakketten aangekondigd. Zo zal Groupe Nethold, die Filmnet in handen heeft, binnenkort een pakket van 150 digitale kanalen introduceren, waarvan er 50 films op aanvraag bieden. BSkyB is voornemens eind 1996 tussen 16 en 32 *pay-per-view* kanalen te introduceren, als eerste stap in de richting van werkelijke video-op-aanvraag-diensten. Canal+ zal binnenkort een pakket van meer dan 20 digitale kanalen aanbieden, dat naast de huidige diensten ook een *pay-per-view* dienst, videospelletjes en digitale radiodiensten zal

---

10 Bron : Europees waarnemingspost voor de audiovisuele sector, *"Statistisch jaarverslag. Cinema, televisie, video en nieuwe media in Europa"*, 1994-1995, Straatsburg 1994.

11 Bron : Europees waarnemingspost voor de audiovisuele sector, *"Statistisch jaarverslag. Cinema, televisie, video en nieuwe media in Europa"*, 1994-1995, Straatsburg 1994, en Libération, *"Les comptes décryptés de Canal+"*, L'évenement, 4.11.1994.

omvatten. Bovendien zal een aantal Franse zenders, waaronder TF1, Arte en La Cinquième, samenwerken om in 1996 een pakket digitale kanalen aan te kunnen bieden via dezelfde satelliet. Ten slotte zal TF1 zelf een pakket diensten introduceren, welke uiteenlopen van video op aanvraag tot interactieve programma's. Hiervoor zullen vijf transponders op Eutelsat worden gebruikt.

Ook nieuwe marktdeelnemers, met name telecommunicatiebedrijven, zullen zich op de markt van diensten van de informatiemaatschappij begeven. British Telecom is reeds een proefproject met 2.500 huishoudens gestart, die op verzoek telewinkeldiensten, video op aanvraag, videospelletjes, enzovoorts kunnen ontvangen.

Momenteel bedienen veel kanalen nog een specifieke geografische markt of taalgebied. Het staat echter vast dat de nationale markten in de toekomst in toenemende mate te beperkt zullen blijken en dat de noodzaak zal toenemen om de grenzen tussen de Lid-Staten te overschrijden. De volgende factoren zijn hiervoor verantwoordelijk :

- *Door de toename van het aantal geëncrypteerde diensten* moeten de marktdeelnemers steeds gerichtere diensten bieden om te voldoen aan de eisen van de markt. Aangezien de marktvraag nog niet op een bevredigende manier wordt bediend, kan een nichemarkt worden gevormd rond een bevolkingslaag die bereid is om te betalen voor deze meerwaarde. Met de uitbreiding van het "algemene" aanbod dat ongecodeerd wordt uitgezonden, hebben de gecodeerde diensten zich ontwikkeld om te voldoen aan een in toenemende mate gespecialiseerde vraag, waarbij het nodig is dat de eindgebruiker een financiële bijdrage levert. De ontwikkeling van deze gerichte diensten op een commercieel haalbare wijze vereist echter een markt van een zekere omvang, en aangezien de markt voor nichediensten in een bepaald geografisch gebied kleiner is dan de markt van een massadienst, *moet een grotere geografische markt worden geëxploiteerd.*

- *De mogelijkheid om beter te voldoen aan taalkundige en culturele vereisten.* Door de toepassing van nieuwe technieken kan eenzelfde zender in diverse talen tegelijk uitzenden middels het gebruik van verschillende geluidsbanden. Bovendien wordt bij het bepalen van de strategie van interactieve diensten in toenemende mate uitgegaan van gespecialiseerde diensten en/of van de levering van dienstenpakketten. De gespecialiseerde diensten spelen vaak in op de vraag van grensoverschrijdende niches, die derhalve op andere factoren dan de nationale cultuur gebaseerd zijn, en de dienstenpakketten stellen de eindgebruiker in staat zelf te kiezen wat hij wil zien. Door de integratie van geavanceerde informatietechnologieën heeft de aanbieder de mogelijkheid een zo breed mogelijk assortiment te bieden door daarin films, programma's of andere diensten op te nemen die beantwoorden aan nationale voorkeuren.

- *De ontwikkeling van technologische toepassingen.* De voortdurende verbetering en voortschrijdende integratie van distributiesystemen voor audiovisuele diensten, die mogelijk worden gemaakt door de commerciële toepassing van nieuwe technologieën (uitzending per satelliet, glasvezel, de ontwikkeling van het ISDN-net (digitaal netwerk voor geïntegreerde diensten) op Europees niveau om IBC-netten (geïntegreerde breedbandcommunicatienetten) tot stand te brengen), maken

deze diensten steeds minder afhankelijk van de afstand tussen de aanbieder en de eindgebruiker.

- Alle regelgevingsactiviteiten die gericht zijn op de *geleidelijke liberalisering* van telecommunicatie (met name per satelliet en kabel) en de *harmonisatie* van de regels van de Lid-Staten inzake het transport van signalen (met name omroep) in Europa (in het bijzonder met betrekking tot de inhoud van de uitzendingen en het auteursrecht) beginnen een positief effect te sorteren op het vrij verrichten van bestaande en in ontwikkeling zijnde audiovisuele diensten, waarvan een groeiend deel geëncrypteerd wordt aangeboden.

- *De ontwikkeling van de praktijk met betrekking tot de toekenning van uitzendrechten :* momenteel kan slechts een beperkt aantal geëncrypteerde kanalen internationaal worden uitgezonden vanwege de traditioneel nationale toekenning van uitzendrechten. Door encryptie zal het in de toekomst mogelijk zijn uitzendrechten te verlenen op basis van het aantal werkelijke ontvangers en niet volgens de nationale grenzen.

- *De optimale exploitatie van de transponders :* aangezien de kosten van transponders hoog zijn, is het voor de exploitant economisch zinvol op zoveel mogelijk gebieden diensten aan te bieden binnen het bereik van de satelliet.

De ontwikkeling van deze diensten om te voldoen aan de groeiende vraag van deze grensoverschrijdende markten wordt echter bedreigd door een belangrijk probleem op Europese schaal : de piraterij.

3. Een markt die met piraterij kampt

3.1. De technologische ontwikkeling

Met geavanceerde technieken is het momenteel in theorie mogelijk een systeem van voorwaardelijke toegang tot stand te brengen dat een dermate hoog veiligheidsniveau biedt, dat eventuele piraten hierdoor ontmoedigd worden. In de praktijk moeten deze systemen echter ook beantwoorden aan de economische en juridische realiteit in de volgende opzichten :

- Zij dienen vervaardigd en gedistribueerd te worden tegen een *redelijke prijs*, omdat de consument slechts bereid is een bepaald maximumbedrag te betalen voor een decoder[12], waarvan de hoogte afhankelijk is van zijn interesse voor de programma's of van het zenderaanbod dat middels dit systeem kan worden ontvangen.

[12] In dit verband hebben bepaalde organisaties die van encryptie gebruik maken ervoor gekozen hun decodeeruitrustingen te verhuren en niet te verkopen, aangezien deze uitrustingen aldus tegen een lagere prijs gedistribueerd kunnen worden en tevens gewaarborgd wordt dat de apparatuur wordt teruggegeven bij het verstrijken van het abonnement.

- De systemen moeten *operationele kosten* met zich meebrengen die niet uitgaan boven het bedrag van de bedreigde opbrengsten, dat wil zeggen de opbrengsten die verloren dreigen te gaan wanneer illegale apparatuur op de markt verschijnt.

- Zij dienen te voldoen aan de *wettelijke voorwaarden* die bepaalde Lid-Staten stellen aan het gebruik van encryptie voor commerciële doeleinden.

Aangezien de kosten van een systeem van voorwaardelijke toegang aanvaardbaar moeten zijn en een onbeperkt veiligheidsniveau tegen illegale ontvangst derhalve niet realiseerbaar is, hebben fabrikanten van illegale decodeeruitrustingen van deze verschuiving geprofiteerd en zijn zij momenteel in staat het tempo van de tecnologische ontwikkeling bij te benen.

De ontwikkeling van de systemen toont dit fenomeen aan. *Het meest eenvoudige systeem* van voorwaardelijke toegang is het scrambelen van de synchronisatiepulsen die deel uitmaken van de uitgezonden signalen, zodat een gewone kijker de horizontale en verticale velden niet in hun oorspronkelijke staat kan terugbrengen. Het beeld wordt normaal uitgezonden, maar omdat synchronisatiepulsen ontbreken, vertoont het scherm slechts een verzameling beeldfragmenten. De voor het herstellen van de synchronisatie benodigde informatie wordt verkapt (algoritme) meegezonden en kan door een decoder worden opgevangen en gebruikt om de noodzakelijke synchronisatiepulsen te herstellen. Dit systeem is reeds veelvuldig nagemaakt[13].

De tweede generatie systemen werkt op een andere manier. Twee encryptiesystemen worden zeer algemeen gebruikt :

- Bij de methode van de *"actieve rotatie van lijnen"* blijven de lijnen op hun plaats, maar worden zij willekeurig doorsneden en worden de laatste delen omgekeerd.

- Bij de methode van de *"vermenging van lijnen"* worden de lijnen die samen het beeld vormen in een volledig andere volgorde opnieuw samengesteld. Deze methode is doelmatiger, maar ook duurder dan de eerste, omdat hierbij een groter aantal gegevens in de decoder moet worden opgeslagen.

Het grote voordeel van deze beide systemen is dat de structuur van het beeld volledig wordt vernietigd. Bovendien kunnen zij worden toegepast in combinatie met een *"smart card"*, een chipkaart die het signaal bij binnenkomst "leest" en aan de decoder de voor decryptie noodzakelijke instructies geeft. Tot deze generatie behoren de drie encryptiesystemen die momenteel het meest gebruikt worden in Europa : Videocrypt, Syster en Eurocrypt.

Het onderzoek naar systemen die nog meer veiligheid bieden wordt echter voortgezet. Door de convergentie die zich voordoet tussen telecommunicatie en audiovisuele diensten en de toepassing van digitale technologie in de omroepwereld kunnen

---

[13] Aangenomen wordt dat de namakers de vertragingsreeks herstellen door de controle van het vertrekpunt te effectueren op de opeenvolgende actieve lijnen. Het technologisch ontwerp van een decoder is enkele jaren geleden zelfs gepubliceerd in de Franse pers.

encryptiesystemen worden ontwikkeld die steeds geavanceerder en veiliger zijn. Ook de ontbinding van de inhoud in digitale bits is op zich reeds een vorm van codering[14].

Om de invoering van interactieve diensten mogelijk te maken, ontwikkelen de decoders zelf zich bovendien in toenemende mate tot "set top boxes", ware computers die worden geactiveerd door een chipkaart waarmee zowel de gebruiker geïdentificeerd wordt als de encryptiefuncties aan de ingang en uitgang van het signaal in werking worden gesteld. Deze uitrustingen kunnen dus het signaal ontvangen, decrypteren, eventueel de inhoud ervan wijzigen, op een ander substraat vastleggen, opslaan en printen. Bovendien zijn zij in staat tot interactie met traditionele apparaten (videorecorders, computers, CD-spelers en nieuwe videodiscs), en kunnen zij het geëncrypteerde signaal, eventueel met vertrouwelijke financiële gegevens, terugzenden naar de exploitant voor de behandeling van de aanvraag.

3.2. De gevolgen van piraterij

De *vervaardiging en verkoop* van decodeerapparaten die niet erkend zijn door de encrypterende organisatie, en de manipulatie van erkende uitrustingen om de ontvangst van de dienst mogelijk te maken in strijd met de voorwaarden betreffende tijd (duur van het abonnement) en hoeveelheid (aantal kanalen) die overeengekomen zijn met de encrypterende organisatie, vormen momenteel in bepaalde Lid-Staten zeer winstgevende activiteiten[15]. Deze activiteiten hebben aldaar bovendien aanleiding gegeven tot parallelle activiteiten, zoals de publikatie van gespecialiseerde tijdschriften en het aanbieden van onderhouds- en servicediensten.

Deze activiteiten, die *de illegale ontvangst van de geëncrypteerde dienst mogelijk maken*, hebben uiteenlopende negatieve gevolgen :

- De encrypterende organisatie loopt de *opbrengsten* mis die zij had kunnen ontvangen indien de kijker een erkende uitrusting had gekocht (ongeveer 200-250 ecu per jaar per illegale ontvanger).

- In bepaalde gevallen moet het *gepirateerde systeem worden vervangen*. Elk jaar geven de exploitanten grote bedragen uit (uit de enquête bij exploitanten kwamen bedragen van ongeveer 60.000 ecu tot meer dan 1.200.000 ecu per jaar per exploitant naar voren) om hun systemen te beschermen (voor controle op de distributie, de verbetering van het systeem, de vervanging van de kaarten, enzovoorts). Zelfs het systeem van controle op afstand met behulp van *smart cards*, dat veiliger leek dan de andere systemen, is niet onaantastbaar gebleken. Men zou kunnen denken dat het bij inbreuk op het systeem zou volstaan de *smart card* te vervangen om het systeem te redden, maar wanneer er een groot aantal abonnees is, kunnen de kosten van vervanging van de kaart de winst van de

---

14 In dit opzicht is de standaardisering van encryptiesystemen voor digitale omroep, die heeft plaatsgevonden in het kader van de werkzaamheden van de *Digital Video Broadcasting Group (DVB)*, een belangrijke stap in de richting van de veralgemenisering van encryptietechnieken en de vergroting van de veiligheid.

15 Geschat wordt dat niet-erkende decodeeruitrustingen momenteel tussen 5 en 20 % van de gehele markt vertegenwoordigen.

onderneming ernstig in gevaar brengen. Naast de kosten van de *smart card* zelf[16] moet immers ook rekening worden gehouden met de kosten van de ontwikkeling van het nieuwe systeem, van voorlichting en van verzending (in dit verband is uit de enquête gebleken dat de kosten van het geheel opnieuw beveiligen van gepirateerde systemen tot meer dan 45.000.000 ecu kunnen bedragen).

- *De tijd die nodig is om een nieuw systeem te ontwikkelen*. Wederom in het voorbeeld van de *smart cards* duurt het enige tijd om een nieuwe kaart te ontwikkelen, wanneer de zender deze moet vervangen. Tijdens deze periode heeft de zender geen andere keuze dan een aantal tijdelijke elektronische tegenmaatregelen te nemen alvorens een andere kaart op de markt kan worden gebracht. Dit is een gevaarlijke situatie, omdat degenen die de inbreuk maken op deze tegenmaatregelen anticiperen en kaarten produceren die inmiddels blijven functioneren. Bovendien is er altijd het probleem van de overlappingsperiode waarin zowel het oude als het nieuwe systeem dienen te werken. Dit brengt met zich mee dat de nagemaakte kaarten die reeds in omloop zijn ook blijven functioneren, waardoor de plegers van de inbreuk de tijd krijgen om nieuwe kaarten te vervaardigen. Momenteel zijn zij zelfs met steun van particuliere investeerders in staat om hun eigen kaarten en chips bijna even snel als de zenders zelf te vervaardigen. Andere technieken om nagemaakte kaarten onbruikbaar te maken (bijvoorbeeld het verzenden van een signaal dat uitsluitend illegale kaarten uitschakelt) zijn slechts kortstondig effectief gebleken (in het onderhavige voorbeeld omdat de illegale vervaardigers op hun beurt uitrustingen maken die speciaal ontworpen zijn om het uitschakelsignaal te blokkeren).

- De schade voor de *rechthebbenden op de programma's* die worden uitgezonden. Aangezien bij de *vergoeding aan de rechthebbenden* doorgaans ook het *potentiële kijkerspubliek* in aanmerking wordt genomen, berooft de ontvangst van geëncrypteerde uitzendingen met illegale uitrustingen deze rechthebbenden van de abonnementsgelden die zij zouden hebben ontvangen indien de bezitter van deze uitrustingen een legale decoder had gekocht. Bovendien hebben de rechthebbenden bij de onderhandelingen over rechten op latere (ongecodeerde) uitzendingen meer moeite een hoge vergoeding te bedingen vanwege de illegale ontvangst die reeds heeft plaatsgevonden tijdens de uitzending door het geëncrypteerde kanaal.

- De inkomstenderving en het verlies aan geloofwaardigheid voor de *leveranciers van de technologie*. Een exploitant die een encryptiesysteem kiest, wil zich ervan vergewissen dat het gekozen systeem het meest veilige is, om de rechthebbenden op de programma's de garantie te kunnen geven dat de uitzending waarvoor zij toestemming hebben gegeven niet illegaal zal worden ontvangen. Een hoog percentage illegale uitrustingen in omloop zou kunnen worden opgevat als een aanwijzing dat het systeem niet goed functioneert.

16 Deze variëren van 5 tot 25 ecu.

- De *ondermijning van het vertrouwen van de markt* in het systeem. De markt moet vertrouwen in encryptie hebben om het idee van exclusiviteit in stand te houden dat met deze diensten geassocieerd wordt, en om het extra uitzendmoment te rechtvaardigen. Dit vertrouwen wordt door de illegale ontvangst in gevaar gebracht, omdat de houders van de rechten terughoudend zullen zijn bij het verlenen van het recht van eerste uitzending, de kanalen geen hoge bedragen zullen willen betalen en de consumenten niet bereid zullen zijn een vergoeding te betalen.

- De consumenten zouden op het moment van aankoop misleid kunnen worden omtrent de herkomst van de decoder en geloven een geautoriseerd apparaat te hebben gekocht, terwijl het in werkelijkheid om een piratendecoder gaat. Als de dienstverrichter in zo'n geval om beveiligingsredenen de versleuteling wijzigt, zal het gekochte apparaat onbruikbaar worden voor de consument, die dan op eigen kosten een andere decoder zal moeten kopen. Bovendien verrekenen de dienstverrichters de verliezen die zij lijden ten gevolge van piraterij in de verkoops- of huurprijs van de door de consument rechtmatig verworven apparatuur.

Naast deze directe gevolgen zijn er ook nog de indirecte gevolgen voor de ontwikkeling van de markt van nieuwe geëncrypteerde diensten. Het is duidelijk dat deze ontwikkeling slechts plaats kan vinden voor zover een adequaat veiligheidsniveau kan worden gegarandeerd. Indien dit niet het geval is, zullen de marktdeelnemers zich terughoudend opstellen ten aanzien van activiteiten die hoge initiële investeringen vergen.

4. Een markt die aan gefragmenteerde regelgeving onderworpen is

Om het hoofd te kunnen bieden aan deze illegale industrie is regelgeving als aanvulling op technologische oplossingen noodzakelijk gebleken, hetgeen aanleiding heeft gegeven tot wetgevingsactiviteiten in de Lid-Staten, die nog immer voortduren en waarbij sterk uiteenlopende benaderingen worden gevolgd. Deze regelingen wordt geanalyseerd in hoofdstuk 3.

De *gefragmenteerde regelgeving* kan evenwel volgens de media-industrie moeilijkheden opleveren voor de ontwikkeling van geëncrypteerde diensten op Europese schaal en in de weg staan aan de goede werking van de interne markt. Aangezien de transnationale dimensie steeds belangrijker wordt voor de groei van een werkelijke Europese industrie van geëncrypteerde diensten, kan het ontbreken van een gelijkwaardig beschermingsniveau tegen piraterij negatieve consequenties hebben voor de ontwikkeling van deze diensten op Europees niveau.

Zoals uit de raadpleging is gebleken, kan het ontbreken van rechtsbescherming in een of meerdere Lid-Staten van ontvangst ertoe leiden dat de marktdeelnemers besluiten om een bepaalde Lid-Staat niet te bedienen, omdat zij de gevolgen van piraterij in die Lid-Staat vrezen. Een doelmatige rechtsbescherming vormt een belangrijke overweging die een marktdeelnemer ertoe kan aanzetten zijn dienst in een Lid-Staat aan te bieden.

Bovendien zijn de noodzakelijke uitgaven voor het onderzoek van de nationale wetgevingen en van mogelijke juridische acties bij piraterij in de verschillende Lid-Staten bijkomende kosten voor de marktdeelnemers, waardoor hun activiteiten duurder worden. Dit heeft weer negatieve gevolgen voor de ontwikkeling van de dienst.

Bij onderhandelingen over de rechten op programma's zal het ontbreken van een gelijkwaardige rechtsbescherming in alle Lid-Staten van ontvangst de verwerving van deze rechten bemoeilijken, omdat de exploitanten met name voor recente produkties niet kunnen garanderen dat de programma's niet illegaal ontvangen zullen worden in andere Lid-Staten. Bovendien wordt de vaststelling van de vergoeding voor de rechthebbenden moeilijker, omdat het onmogelijk is met zekerheid de omvang van het publiek in het gehele ontvangstgebied van het signaal te bepalen. De exploitanten zullen daarom meer moeite hebben om de rechten tegen redelijke prijzen te kopen, hetgeen zijn weerslag zal hebben op de ontwikkeling van hun diensten, en met name van hun grensoverschrijdende diensten.

Aangezien bepaalde wijzen van uitzending gevoeliger zijn voor illegale ontvangst dan andere (met name de uitzending via de ether of per satelliet ten opzichte van de distributie per kabel, die in het algemeen veiliger is in verband met de fysieke verbinding met de kijker), kunnen de exploitanten ervoor kiezen bepaalde methoden niet te gebruiken omdat zij het gevaar van piraterij te hoog achten. Indien een doelmatige rechtsbescherming ontbreekt, zullen bepaalde wijzen van uitzending, met name die welke veel grensoverschrijdende mogelijkheden bieden, minder gebruikt worden dan andere.

Het ontbreken van een gelijkwaardige rechtsbescherming in de Lid-Staten heeft bovendien negatieve gevolgen in het geval van invoer van illegale uitrustingen uit derde landen. Deze uitrustingen kunnen de Gemeenschap binnenkomen via een Lid-Staat die geen verbod kent op de verkoop en distributie daarvan, en vervolgens gemakkelijk in andere Lid-Staten in omloop komen. De bestrijding van de illegale ontvangst in deze andere Lid-Staten loopt daardoor het gevaar haar doelmatigheid te verliezen.

De verschillen tussen de regels die van toepassing zijn op de illegale ontvangst kunnen daarnaast leiden tot vervalsing van de mededingingsvoorwaarden voor de marktdeelnemers uit verschillende landen. De marktdeelnemers die uitzenden in landen die een goede rechtsbescherming bieden, hebben een concurrentievoordeel (dat doorwerkt in hun vermogen om programma's aan te kopen) ten opzichte van de marktpartijen die uitzenden in een land waar geen sprake is van rechtsbescherming, omdat deze laatste de aanvullende kosten moeten dragen van bijvoorbeeld een extra veilig encryptiesysteem.

Ten slotte bestaat door de uiteenlopende regels in de Lid-Staten het gevaar dat de mogelijkheden die de richtlijn inzake het gebruik van normen voor het uitzenden van televisiesignalen[17] biedt, niet benut zullen worden. Het gebruik van in toenemende mate gestandaardiseerde systemen zal belemmerd worden door het feit dat het niveau van de rechtsbescherming tegen illegale ontvangst niet in alle Lid-Staten gelijk is. Het veiligheidsniveau van het systeem en van de wijzen van distributie van de decodeeruitrustingen zal variëren met de Lid-Staat van ontvangst, waardoor opnieuw

[17] Genoemde Richtlijn 95/47.

fragmentatie optreedt in een audiovisuele ruimte die in zekere mate gestandaardiseerd zou moeten zijn. In dit opzicht heeft de *Digital Video Broadcasting Group (DVB)*, die aan de basis staat van de standaardisering van de normen voor digitale televisie, welke deels overgenomen zijn in Richtlijn 95/47, een aanbeveling vastgesteld waarin de noodzaak wordt benadrukt van een helder en uniform regelgevingskader op unieniveau, waarop de exploitanten kunnen vertrouwen in het geval van illegale ontvangst van geëncrypteerde diensten.

HOOFDSTUK 2 : DE INTERNATIONALE REGELGEVING

1. De werkzaamheden in het kader van de Raad van Europa

De Raad van Europa heeft in september 1991 een Aanbeveling aan de Lid-Staten vastgesteld over de *rechtsbescherming van geëncrypteerde omroepdiensten*[18]. Deze aanbeveling werd vervolgens bijgewerkt middels een andere aanbeveling inzake maatregelen tegen audio- en videopiraterij, welke in januari 1995 werd vastgesteld[19].

In de preambule onderstreept de Raad de voordelen die de invoering in Europa van betaalomroepdiensten opleveren, met name voor de sector produktie van audiovisuele werken. De Raad erkent dat geëncrypteerde omroepdiensten bijdragen tot een grotere diversiteit van het programma-aanbod voor het publiek, de exploitatiemogelijkheden van beschermde werken uitbreiden en de financiering van de produktie van werken en programma's in Europa bevorderen, omdat encryptie de zenders extra inkomsten oplevert.

Vervolgens wordt in de aanbeveling het licht geworpen op de negatieve gevolgen van de illegale toegang tot geëncrypteerde omroepdiensten, en wordt een opsomming gegeven van de activiteiten die als illegaal moeten worden beschouwd. Het gaat hierbij met name om :

- de vervaardiging van decodeeruitrustingen om de toegang tot geëncrypteerde diensten mogelijk te maken voor personen die niet tot het door de encrypterende organisatie bepaalde publiek behoren;

- de invoer van decodeeruitrustingen om de ontvangst van geëncrypteerde uitzendingen mogelijk te maken voor personen die niet tot het door de encrypterende organisatie bepaalde publiek behoren;

- de distributie van decodeeruitrustingen om de toegang tot geëncrypteerde diensten mogelijk te maken voor personen die niet tot het door de encrypterende organisatie bepaalde publiek behoren;

- het maken van promotie en reclame voor de vervaardiging, invoer of distributie van dergelijke decodeeruitrustingen;

- het bezit voor commerciële doeleinden van decodeeruitrustingen die de toegang tot omroepdiensten mogelijk maken voor personen die niet tot het door de encrypterende organisatie bepaalde publiek behoren.

De Lid-Staten kunnen bepalen dat het bezit voor privégebruik ook tot de illegale activiteiten behoort.

---

18 Aanbeveling nr. R(91) 14 van het Comité van Ministers aan de Lid-Staten over de rechtsbescherming van geëncrypteerde omroepdiensten.

19 Aanbeveling nr. R(95) 1 van het Comité van Ministers aan de Lid-Staten over maatregelen tegen audio- en videopiraterij.

Daarna worden *geëncrypteerde diensten* in de aanbeveling gedefinieerd als elke televisiedienst die wordt uitgezonden of heruitgezonden op ongeacht welke technische wijze, waarvan de kenmerken worden gewijzigd of veranderd ten einde de toegang tot deze dienst tot een bepaald publiek te beperken. In de toelichting benadrukt de Raad dat deze definitie (en de bescherming die daaruit voortvloeit) van toepassing is op alle organisaties die geëncrypteerde diensten aanbieden, of dit nu op plaatselijk, regionaal, nationaal of transnationaal niveau geschiedt, en ongeacht het land van oorsprong van de uitzending.

Aan de door de Raad van Europa gegarandeerde bescherming kleeft derhalve geen enkele wederkerigheidsvoorwaarde. Zoals de Raad eveneens in zijn toelichting heeft beklemtoond, zou de uitsluiting van diensten uit bepaalde landen van de bescherming problemen kunnen opleveren voor de diensten die afkomstig zijn uit het land van ontvangst.

De aanbeveling definieert *decodeeruitrustingen* als elk apparaat en elke uitrusting of inrichting die geheel of gedeeltelijk ontworpen of aangepast is om de ongecodeerde toegang tot een geëncrypteerde dienst, dat wil zeggen zonder wijziging of verandering van de kenmerken daarvan, mogelijk te maken[20].

Ten slotte wordt *distributie* gedefinieerd als de verkoop, verhuur of commerciële installatie van een decodeeruitrusting, alsmede het bezit van een decodeeruitrusting met het oog op deze activiteiten. Deze definitie heeft derhalve uitsluitend betrekking op commerciële activiteiten en niet op privé-activiteiten.

Met betrekking tot de *sancties* spoort de aanbeveling de Lid-Staten aan strafrechtelijke of administratieve sancties vast te stellen voor alle genoemde gedragingen, evenwel met één uitzondering : reclame of promotie voor de vervaardiging, invoer of distributie van illegale uitrustingen leidt niet tot strafrechtelijke of administratieve sancties[21].

De in de aanbeveling voorgestelde *civiele rechtsmiddelen* betekenen dat, afgezien van de strafrechtelijke sancties, de benadeelde encrypterende organisatie een actie bij de rechter kan instellen om schadevergoeding of een percentage van de winst te eisen.

De rechthebbenden op de programma's die deel uitmaken van de dienst beschikken in dit opzicht niet over rechtsmiddelen. De Raad merkt in de toelichting op dat, hoewel de rechthebbenden op de uitgezonden programma's schade ondervinden van het gebruik van illegale uitrustingen, deze schade een indirect karakter heeft ten opzichte van de schade

---

20 In de toelichting verklaart de Raad dat de beginselen van de aanbeveling uitsluitend van toepassing dienen te zijn op het gedeelte van de decoder dat de decryptie van het signaal mogelijk maakt. Zo is in een systeem waarbij *smart cards* worden gebruikt het relevante gedeelte uitsluitend de kaart, en niet de decoder op zich, omdat het signaal niet gedecodeerd kan worden met de decoder alleen.

21 De Raad rechtvaardigt deze uitzondering met het argument dat de sancties uitsluitend moeten gelden voor degenen die illegale uitrustingen vervaardigen, invoeren en distribueren, en niet voor organisaties die louter reclame- en promotie-activiteiten uitvoeren (reclamebureaus, dagbladen en tijdschriften).

(4)

die de zenders lijden. Bovendien vermeldt het verslag dat de rechthebbenden de bescherming van hun rechten zeker kunnen stellen via contractuele clausules, waarin wordt bedongen dat de zenders in het geval van piraterij een gerechtelijke actie moeten instellen[22].

Ten slotte bevat de aanbeveling geen strafrechtelijke of administratieve sancties op het bezit voor privédoeleinden.

Deze aanbeveling heeft een belangrijke rol gespeeld bij de regelgeving die begin jaren negentig in de Lid-Staten is vastgesteld. De specifieke nationale voorschriften inzake de rechtsbescherming van geëncrypteerde omroep zijn vaak geënt op de in de aanbeveling vervatte beginselen.

Door de aard zelf van deze tekst, die geen dwingend karakter heeft, lopen deze voorschriften evenwel aanzienlijk uiteen, met name wat betreft het toepassingsgebied, de verboden activiteiten en de strafmaat. Anderzijds hebben diverse Lid-Staten van de Europese Unie de beginselen van de aanbeveling nog niet omgezet in nationale wetgeving. Dit heeft geleid tot de huidige fragmentatie van de regelgeving op Europees niveau.

2. De werkzaamheden in het kader van de WIPO

In het kader van de lopende besprekingen over het ontwerp-protocol bij de Berner Conventie en het Nieuwe Instrument voor de bescherming van de rechten van producenten en uitvoerders van fonografische werken wordt in hoofdstuk IX inzake sancties van het ontwerp-memorandum, dat in april 1994[23] door het Bureau is opgesteld, voorgesteld de mogelijkheid te bestuderen om bepalingen vast te stellen over misbruik van technische middelen.

In dit opzicht is voorgesteld met een inbreuk op het auteursrecht gelijk te stellen de vervaardiging, invoer en distributie, met het oog op verhuur en verkoop, van elke inrichting die bestemd is om de ontvangst van een gecodeerd programma, dat is uitgezonden of op enige andere wijze aan het publiek is doorgegeven, mogelijk te maken of te vergemakkelijken voor personen die daartoe niet bevoegd zijn.

Bovendien kunnen de rechthebbenden op programma's die gedecrypteerd worden met een illegale uitrusting een actie tot schadevergoeding instellen.

---

22 Hoewel de rechthebbenden dergelijke bedingen in de contracten kunnen laten opnemen, neemt dit niet weg dat het noodzakelijk blijft de belangen die eigen zijn aan de rechthebbenden onafhankelijk van die van de zenders te beschermen. Wanneer de illegale activiteit niet de zender, maar wel de rechthebbenden benadeelt, heeft de zender er mogelijk geen belang bij om snel tegen deze activiteit op te treden. De rechthebbenden zouden dan weliswaar een procedure kunnen instellen tegen de zender om nakoming van de contractuele verplichtingen af te dwingen die hij bij het sluiten van het contract aanvaard heeft, maar dit levert slechts vertraging op voor de actie tegen degene die de rechthebbenden benadeelt.

23 Document OMPI 9099D/COP/0691D van 29 april 1994.

Aangezien de onderhandelingen over deze teksten nog niet zijn afgerond, is het voorbarig om een uitspraak te doen over de mogelijkheid deze voorstellen in de uiteindelijke tekst op te nemen. Opgemerkt dient echter te worden dat in dit geval het toepassingsgebied niet beperkt is tot omroep, maar zich uitstrekt tot elke doorgifte aan het publiek van het beschermde werk.

HOOFDSTUK 3 : DE WETGEVING VAN DE LID-STATEN

1. Algemeen

De analyse van de stand van de wetgeving heeft betrekking op de oplossingen die in de nationale voorschriften zijn nagestreefd voor het probleem van de *illegale ontvangst van een geëncrypteerde dienst*, dat wil zeggen, de ontvangst zonder betaling en/of toestemming door personen die daartoe niet zijn gemachtigd door de verrichter van de diensten.

In het navolgende wordt een uitvoerige analyse gemaakt van de oplossingen die in de nationale wetgeving van elke Lid-Staat zijn gekozen voor het probleem van de illegale ontvangst van een geëncrypteerde dienst, evenwel met de kanttekening dat de stand van de wetgeving zeer snel evolueert en elke "momentopname" derhalve het gevaar loopt op korte termijn achterhaald te worden.

2. De stand van de wetgeving in de Lid-Staten (algemeen overzicht)

Er is in Europa momenteel geen sprake van een eenvormige en systematische aanpak van de problemen die veroorzaakt worden door de illegale ontvangst van geëncrypteerde diensten. In bepaalde landen bestaan *specifieke rechtsvoorschriften*, in andere landen wordt gebruik gemaakt van *reeds bestaande bepalingen* en in weer andere landen zijn *in het geheel geen rechtsmiddelen* voorhanden om de bescherming te waarborgen.

In dit verband moet erop worden gewezen dat de richtlijn "Kabel en satelliet"[24] weliswaar heeft geleid tot de harmonisatie van de behandeling van beschermde werken die worden uitgezonden per satelliet en doorgegeven via de kabel in de Gemeenschap, maar de marktdeelnemers geen enkele steun biedt in hun strijd tegen illegale ontvangst.

Houders van rechten kunnen inderdaad, in bepaalde omstandigheden, de niet-gemachtigde heruitzending van hun werken verhinderen; dit geldt echter niet voor niet-gemachtigde ontvangst. Dit is zo omdat dit geen relevante handeling is in het auteursrecht, dat zich beperkt tot traditionele communicatie en niet de ontvangst van een beschermd werk afdekt. Dientengevolge zal de nationale regelgeving, die de Richtlijn omzet, niet bruikbaar zijn bij het voorkomen van de illegale ontvangst van vercijferde diensten.

---

[24] Eerdergenoemde Richtlijn 93/83/EEG.

Tabel I : Wetgeving inzake de bescherming van geëncrypteerde diensten

wetgeving	specifiek				algemeen	
	omroep	telecom.	intellectuele eigendom	strafrecht	oneerlijke concurrentie	intellectuele eigendom
Oostenrijk					x	
België		x			x	
Denemarken						
Finland		x				
Frankrijk	x			x		
Duitsland					x	
Griekenland						
Ierland	x					
Italië	x					
Luxemburg						
Nederland				x	x	
Portugal						
Spanje						x
Zweden				x		
Verenigd Koninkrijk	x		x			

2.1. Toepassing van de bepalingen inzake oneerlijke concurrentie en intellectuele eigendom

In landen waar specifieke regelgeving ontbreekt, wordt vaak *andere, meer algemene regelgeving* toegepast, die bescherming biedt tegen oneerlijke handelspraktijken. Dit heeft er in bepaalde gevallen toe geleid dat de vervaardiging, invoer en in de handel brengen (verkoop, verhuur, bezit met commerciële doeleinden) van illegale uitrustingen verboden werd (A, B, D, NL).

Deze maatregelen zijn meestal gebaseerd op het feit dat de vervaardiging en verkoop van niet door de encrypterende organisatie erkende uitrustingen deze organisatie berooft van de *beloning* die doorgaans verschuldigd is voor de geleverde prestatie. De niet-erkende fabrikant ontvangt immers een beloning voor een prestatie (de ontvangst van de dienst) die door een ander geleverd is.

Het bestaan van concurrentie tussen de organisaties die encrypteren en de niet-erkende fabrikanten, een voorwaarde voor toepassing van de regels inzake oneerlijke concurrentie, is in bepaalde gevallen aanvaard[25]. Hiertoe is het echter noodzakelijk dat de belanghebbende partij daadwerkelijk op de markt aanwezig is. Wanneer een te beschermen handelsbelang ontbreekt, zijn de beginselen van oneerlijke concurrentie niet van toepassing.

Bovendien kan een actie op basis van oneerlijke concurrentie doorgaans slechts worden ingesteld tegen de distributie van en het maken van reclame voor niet-erkende decodeeruitrustingen, en niet tegen de invoer en het bezit daarvan. Dit houdt in dat het moeilijk is om op te treden voordat de uitrusting in de handel is gebracht, en dat niet om preventieve maatregelen kan worden verzocht.

---

25 In dit verband heeft het Oostenrijkse Hof (in zaak Teleclub/Olbort) uitdrukkelijk erkend dat er geen sprake hoeft te zijn van daadwerkelijke concurrentie, omdat de goederen naar hun aard reeds onderling concurreren.

Het is ook moeilijk gebleken gebruik te maken van andere algemene regelgeving. Bij de niet-erkende vervaardiging van decodeeruitrustingen biedt het intellectuele-eigendomsrecht de rechthebbenden een zekere bescherming, omdat op diverse componenten van de uitrusting intellectuele of industriële eigendomsrechten kunnen rusten.

Een dergelijke actie is evenwel vaak ondoelmatig gebleken. Om te bewijzen dat een *smart card* een kopie is van de software van de eigenaar van het systeem, moet tijdens het rechtsgeding het encryptie-algoritme onthuld worden en komt de gebruikte technologie aan het licht, zodat de weg naar andere kopieën geopend wordt. Anderzijds gaat het soms om legale kaarten die op frauduleuze wijze opnieuw geactiveerd worden na het verstrijken van de geldigheidsduur. In dit geval is een actie op basis van de intellectuele eigendomsrechten op de kaart zinloos.

Overigens beschikken de organisaties die van encryptie gebruik maken niet altijd over dit rechtsmiddel tegen fabrikanten van illegale uitrustingen, omdat zij niet altijd eigenaar zijn van de betrokken intellectuele eigendomsrechten.

2.2. Toepassing van specifieke regelgeving

De *specifieke wetgeving* betreffende de bescherming van geëncrypteerde diensten tegen illegale ontvangst is een zeer recent fenomeen, dat volgde op de technologische ontwikkeling die de telecommunicatiewereld sinds het einde van de jaren zeventig heeft doorgemaakt. Naar aanleiding van de grote hoeveelheid illegale uitrustingen die op de markt verscheen van landen waar de geëncrypteerde omroep het meest ontwikkeld was (F, VK), zag de eerste wetgeving het licht in 1987 (F) en 1988 (VK).

Een tweede beweging deed zich voor in het begin van de jaren negentig, met de expansie van de geëncrypteerde kanalen in Europa in Ierland, België (1991), Italië (1992), Finland en Zweden (1994). Deze tweede beweging is nog niet geëindigd, zoals blijkt uit het debat dat in Denemarken wordt gevoerd over de indiening van een wetsontwerp.

In landen waar sprake is van regelgeving, heeft deze meestal de vorm gekregen van een *bijzondere wet inzake de audiovisuele industrie*. Voor de strafbaarstelling van bepaalde activiteiten in verband met de illegale ontvangst van geëncrypteerde diensten en voor de verlening aan exploitanten, en in bepaalde gevallen ook aan andere belanghebbenden, van een recht op schadevergoeding en intrest ten opzichte van de verantwoordelijken voor deze activiteiten is houvast gezocht bij de auteurswetgeving.

Op basis hiervan kan de situatie met betrekking tot de bestaande nationale regelgeving inzake de bescherming van geëncrypteerde diensten als volgt worden samengevat :

2.2.1. Het voorwerp van de maatregelen : de bescherming van geëncrypteerde diensten tegen illegale ontvangst

Hoewel de nationale regels geen eenvormige definitie geven van illegale ontvangst, die nu eens wordt omschreven als *de ontvangst van betaalprogramma's zonder dat betaling heeft plaatsgevonden* (B, F, VK), dan weer als *de toegang tot een geëncrypteerde dienst zonder toestemming van de encrypterende organisatie* (S, I), hebben zij alle hetzelfde

doel : *waarborgen dat slechts degenen die daarvoor toestemming hebben de dienst kunnen ontvangen*.

Er bestaat echter een *verschil* tussen de regels die *uitsluitend van toepassing zijn op omroepdiensten* en op de doorgifte via de kabel, waarbij hetzelfde programma aan het algemene publiek wordt doorgegeven (I, F, B, IRL, S), en die welke ook betrekking hebben op *informatiediensten die op individueel verzoek via het net worden verstrekt* (SF, VK, NL). Deze laatste regels maken geen onderscheid tussen diensten die aan het grote publiek worden doorgegeven en diensten die op verzoek worden geleverd.

Wanneer rechtsbescherming tegen de illegale ontvangst van geëncrypteerde omroepdiensten wordt geboden, geldt deze bescherming doorgaans voor alle omroepsignalen, maar niet altijd voor alle radiodiensten. Bepaalde landen (VK, IRL) stellen een dergelijke bescherming ook afhankelijk van de *oorsprong* (nationaal of uit het buitenland) of van *de wijze van uitzending van de dienst* (per satelliet of via de ether).

Tabel II : Beschermde diensten (naar type)

Beschermde diensten	omroep			radio	overige	tegen betaling
	kabel	satelliet	overige			
Oostenrijk						
België	x	x	x			x
Denemarken						
Finland	x	x	x	x	x	
Frankrijk	x	x	x			x
Duitsland						
Griekenland						
Ierland	x					x
Italië	x	x	x	x		
Luxemburg						
Nederland	x	x	x	x	x	x
Portugal						
Spanje						
Zweden	x	x	x	x		x
Verenigd Koninkrijk	x	Uitsluitend voor uit het VK afkomstige diensten	x	x	x	x

Voor de bescherming van de aanbieders van de diensten tegen de ontvangst door personen die daartoe niet gemachtigd zijn, zijn in de nationale voorschriften *twee benaderingen* gevolgd.

De eerste is *de bescherming van de geëncrypteerde dienst*. Gewoonlijk wordt hierbij erkend dat de encrypterende organisatie de *eigendom van het signaal* heeft. De ontvangst van het signaal zonder instemming wordt dan beschouwd als "diefstal", waartegen de eigenaar, de encrypterende organisatie, bescherming kan verlangen (Franse gemeenschap van België, IRL, I, VK, NL, SF). Bijkomend verbiedt wetgeving van dit type soms de heruitzending, onderschepping en daarmee verbonden activiteiten, voor zover deze de illegale ontvangst van het signaal mogelijk maken en/of vergemakkelijken.

Tabel III : Verboden handelingen

Geëncrypteerde omroepdiensten	onderschepping	gebruik	uitzending	ontvangst door derden organiseren/mogelijk maken
Oostenrijk				
België*	x		x	x
Denemarken				
Finland		x		
Frankrijk		x	x	x
Duitsland				
Griekenland				
Ierland	x			x
Italië	x		x	
Luxemburg				
Nederland		x		
Portugal				
Spanje				
Zweden				x
Verenigd Koninkrijk	x	x		x

* ***Uitsluitend de Franse gemeenschap***

In de tweede benadering wordt de aandacht rechtstreeks gericht op de noodzaak *voorbereidende handelingen* te verbieden (Vlaamse gemeenschap van België, F, S). De illegale ontvangst op zich wordt niet langer beschouwd als een verboden activiteit, maar de *handelsactiviteiten die deze vergemakkelijken* wel.

Een dergelijk verschil in benadering heeft gevolgen voor de reikwijdte van de bescherming. De wetgeving die de benadering van de bescherming tegen diefstal van het signaal volgt, verbiedt doorgaans de voorbereidende activiteiten, of deze nu met commercieel oogmerk of voor privé-doeleinden verricht worden. Regelingen die zich uitsluitend richten op de voorbereidende activiteiten, strekken zich evenwel niet uit tot gedragingen van particulieren.

Tabel IV : doel van de illegale activiteiten met betrekking tot decodeeruitrustingen

Doel	commercieel	niet-commercieel
Oostenrijk		
België	x	x
Denemarken		
Finland	x	x
Frankrijk	x	x
Duitsland		
Griekenland		
Ierland	x	x
Italië	x	
Luxemburg		
Nederland	x	x
Portugal		
Spanje		
Zweden	x	
Verenigd Koninkrijk	x	x

De voorbereidende activiteiten, die, naargelang het geval, een aanvulling vormen op het verbod van ontvangst of het specifieke voorwerp van de wetgeving zijn, kunnen betrekking hebben op :

a) *De vervaardiging van decodeeruitrustingen* die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

Om ervoor te zorgen dat de particulieren het programma uitsluitend met behulp van door de encrypterende organisatie zelf of voor zijn rekening vervaardigde uitrustingen kunnen ontvangen, verbieden alle regelingen de vervaardiging van uitrustingen die uitsluitend bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling van een vergoeding mogelijk te maken (B, F, I, S, SF, NL, VK, IRL).

b) *De invoer van decodeeruitrustingen* die bestemd zijn om de ontvangst van een geëncrypteerde dienst mogelijk te maken zonder betaling.

Met de voortschrijdende opheffing van de controle aan de grenzen is het gevaar groter geworden dat niet-erkende uitrustingen, die vervaardigd zijn in een Lid-Staat waar geen verbod op vervaardiging bestaat, worden ingevoerd om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken. Met het oog hierop verbiedt de wetgeving in bepaalde landen (B, F, I, VK, SF, IRL) de invoer van decodeeruitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

c) *De distributie van decodeeruitrustingen* die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

De activiteit die de meeste schade toebrengt aan de activiteiten van de aanbieders van geëncrypteerde diensten is ongetwijfeld het in de handel brengen van uitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken. Daarom verbiedt de wetgeving doorgaans de distributie van dergelijke decodeeruitrustingen (B, F, I, S, VK, IRL, SF, NL).

d) *Bezit voor commerciële doeleinden* van decodeeruitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

Het bezit voor commerciële doeleinden, met name met het oog op de verkoop en/of verhuur is een andere fase in de frauduleuze activiteit die leidt tot de ontvangst van een geëncrypteerde dienst zonder betaling van een vergoeding. Derhalve verbiedt de wet in bepaalde landen (B, F, I, IRL, SF, NL) het bezit voor commerciële doeleinden van decodeeruitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

e) *Bezit voor privédoeleinden* van decodeeruitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

Hoewel het bezit voor privédoeleinden van een decodeeruitrusting die bestemd is om de ontvangst van een geëncrypteerde dienst mogelijk te maken zonder betaling op zich een minder ernstige activiteit is dan het bezit voor commerciële doeleinden, hebben bepaalde landen (B, F, I, IRL, SF, NL) geoordeeld dat zelfs het bezit door een particulier van een niet-erkende uitrusting verboden moet worden.

f) *Reclame* voor decodeeruitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

Aangezien met de regelgeving wordt beoogd de aanbieder van de dienst tegen illegale ontvangst te beschermen, verbieden bepaalde landen (B, F, VK, IRL. NL, I) ook reclame-activiteiten voor uitrustingen die bestemd zijn om de ontvangst van een geëncrypteerde dienst zonder betaling mogelijk te maken.

Tabel V : Illegale activiteiten met betrekking tot decodeeruitrustingen

decodeer-uitrusting	vervaardiging	invoer	distributie	reclame	bezit voor commerciële doeleinden	détention à des fins privatives
Oostenrijk						
België*	x	x	x	x	x	x
Denemarken						
Finland	x	x	x		x	x
Frankrijk	x	x	x	x	x	x
Duitsland						
Griekenland						
Ierland	x	x	x	x	x	x
Italië	x	x	x	x	x	x
Luxemburg						
Nederland	x		x	x	x	x
Portugal						
Spanje						
Zweden	x		x			
Verenigd Koninkrijk	x	x	x	x		

** Uitsluitend de Vlaamse gemeenschap*

Overigens hebben de meeste Lid-Staten ook andere, bijkomende activiteiten verboden die alle in verband staan met het in de handel brengen van decodeeruitrustingen.

Tabel VI : Andere illegale activiteiten in verband met decodeeruitrustingen

Decodeer-uitrustingen	aanpassing	verkoop	verhuur	installatie	onderhoud	gebruik	aankoop	autres
Oostenrijk								
België		x	x	x			x	
Denemarken								
Finland						x		
Frankrijk		x		x			x	
Duitsland								
Griekenland								
Ierland				x	x			
Italië		x	x					
Luxemburg								
Nederland								
Portugal								
Spanje								
Zweden		x	x	x	x			
Verenigd Koninkrijk		x	x					

2.2.2. Sancties

De nationale rechtsvoorschriften bevatten doorgaans *strafrechtelijke of administratieve sancties* bij schending van de wet, alsmede de mogelijkheid om in een civiele procedure *schade en intresten* te vorderen. Met betrekking tot dit laatste punt kunnen zich verschillende varianten voordoen :

Allereerst kan elke verwijzing naar een actie tot vergoeding van schade en intresten ontbreken, hetgeen gewoonlijk inhoudt dat de algemene regels van toepassing zijn (B, F, I, NL).

Ten tweede kan specifiek worden verwezen naar regels die van toepassing zijn op de acties tot vergoeding van schade en intresten, zoals in het Deens wetsontwerp. In de toelichting bij het voorstel wordt opgemerkt dat de aanbieders van de diensten en de rechthebbenden op de uitzending schadevergoeding en intresten moeten kunnen eisen voor het verlies dat is geleden door de activiteiten van niet-erkende fabrikanten.

Een derde mogelijkheid is dat een bepaling is vastgesteld dat de rechtsmiddelen waarover de rechthebbenden op het auteursrecht beschikken van toepassing zijn (VK). Dit omvat de mogelijkheid een vergoeding te eisen voor schade en intresten, en het recht de beëindiging van de frauduleuze activiteit te vorderen. Ten slotte kan er sprake zijn van wetgeving waarin de specifieke civiele rechtsmiddelen zijn vastgesteld en de mogelijke eisers en typen acties worden genoemd (IRL).

Tabel VII: sancties

Sancties	boete	gevangenisstraf	administratieve bepalingen	civiele bepalingen
Oostenrijk				
België	26 tot 100 000 BEF (0,7 tot 2 650 ecu)	-	verbeurdverklaring van decodeermaterieel en behaalde winsten	-
Denemarken				
Finland	boete	maximaal 2 jaar	inbeslagname van materieel en verbeurdverklarig van behaalde winsten	-
Frankrijk	5 000 tot 200 000 FF (772 tot 30 880 ecu)	maximaal 2 jaar	inbeslagname van technische gegevens, inbeslagname en verbeurdverklaring van de uitrusting en van reclamemateriaal, verbeurdverklaring van behaalde winsten	
Duitsland		-		-
Griekenland				
Ierland	maximaal 20 000 IEP (24 554 ecu)	maximaal 2 jaar	inbeslagname en verbeurdverklaring van in het kader van delict gebruikt materieel	specifieke rechtsmiddelen
Italië	500 000 tot 6 000 000 ITL (220 tot 2 645 ecu)	3 maanden tot 3 jaar	-	-
Luxemburg				
Nederland	maximaal 100 000 NLG (48 670 ecu)	maximaal 3 jaar	verbeurdverklaring van goederen en van behaalde winsten	-
Portugal				
Spanje				
Zweden	boete	maximaal 6 maanden	verbeurdverklaring van voorwerpen en materieel en van behaalde winsten	-
Verenigd Koninkrijk	maximaal 5 000 GBP (6 045 ecu)	maximaal 2 jaar	vordering op basis van auteursrecht	vordering op basis van auteursrecht

2.2.3. Het uiteenlopend karakter van de maatregelen :

Uit het voorgaande blijkt dat de bestaande regelingen in de Lid-Staten sterk uiteenlopen. Deze verschillen bestaan met name ten aanzien van :

- het toepassingsgebied (nationale of uit andere Lid-Staten afkomstige diensten, omroepdiensten of elke geëncrypteerde dienst, met inbegrip van diensten op individuele aanvraag);

- de mate van bescherming (verbod van bezit voor privédoeleinden en van reclame);

- degenen die een civiele procedure kunnen instellen (encrypterende organisatie of elke belanghebbende)

- de strafmaat.

Deze verschillen doen zich nog duidelijker gelden waar specifieke regelgeving ontbreekt.

Conclusie

Bepaalde Lid-Staten hebben sinds het einde van de jaren tachtig specifieke regelgeving vastgesteld om de bescherming van geëncrypteerde diensten tegen illegale ontvangst met niet-erkende decodeeruitrustingen te waarborgen. Andere Lid-Staten passen met het oog op deze zelfde bescherming algemene, reeds bestaande bepalingen toe (oneerlijke concurrentie, intellectueel eigendomsrecht). Bepaalde Lid-Staten ten slotte bieden een dergelijke bescherming momenteel niet.

Hieruit vloeit voort dat de juridische benaderingen van de illegale ontvangst van een geëncrypteerde dienst binnen de Europese Unie sterk uiteenlopen. Bepaalde activiteiten die verboden zijn in bepaalde Lid-Staten kunnen rechtmatig zijn in andere Lid-Staten.

Vraag 1 : De Commissie zou gaarne aanvullende gegevens ontvangen om een uitvoeriger analyse van de vastgestelde nationale regelgeving te kunnen maken.

HOOFDSTUK 4 : DE BELEMMERINGEN VOOR DE GOEDE WERKING VAN DE INTERNE MARKT

In het licht van de situatie met betrekking tot de regelgeving in de Lid-Staten is de Commisie van mening dat de huidige fragmentatie kan leiden tot belemmeringen voor het vrije verkeer van goederen en diensten en derhalve afbreuk kan doen aan de *goede werking van de interne markt*.

Bepaalde belemmeringen lijken onverenigbaar met de beginselen van het Verdrag en moeten dus worden weggenomen. Dit is in de eerste plaats het geval met bepaalde nationale voorschriften die voor de bescherming tegen illegale ontvangst een onderscheid maken naar *de herkomst van de dienst*. Deze regels bepalen soms dat de uit andere Lid-Staten afkomstige diensten slechts zijn beschermd tegen illegale ontvangst wanneer de nationale autoriteit van tevoren een *verklaring heeft afgegeven dat deze diensten voor bescherming in aanmerking komen*[26].

Andere voorschriften sluiten bepaalde diensten van bescherming uit wegens de *wijze van uitzending*. Dit is bijvoorbeeld het geval wanneer uitsluitend de diensten via de ether of de kabel zijn beschermd tegen illegale ontvangst, en geëncrypteerde diensten per satelliet, welke alle uit het buitenland afkomstig zijn, niet[27]. Hierbij is sprake van verkapte discriminatie.

In deze gevallen wordt de verrichting van grensoverschrijdende diensten, zoals die tussen de abonnee en de encrypterende organisatie, moeilijker gemaakt dan de verrichting van nationale diensten. Deze laatste genieten immers automatisch bescherming, terwijl de uit andere Lid-Staten afkomstige diensten niet of eerst na afgifte van een verklaring beschermd zijn. Deze maatregelen lijken niet gerechtvaardigd in het licht van de jurisprudentie van het Hof van Justitie van de Europese Gemeenschappen. Discriminerende maatregelen die van toepassing zijn op dienstverrichtingen zijn immers slechts verenigbaar met het gemeenschapsrecht indien zij kunnen vallen onder een uitdrukkelijk afwijkende bepaling, zoals artikel 56 van het Verdrag, dat betrekking heeft op de openbare orde, openbare veiligheid en volksgezondheid[28]. In het onderhavige geval lijkt geen der genoemde redenen een dergelijk onderscheid te kunnen rechtvaardigen. In dit verband *kan de Commissie in het kader van het toezicht op de toepassing van het gemeenschapsrecht een einde maken aan dergelijke vormen van discriminatie*.

Bij de analyse van de nationale rechtsregels zijn echter ook een zeker aantal *belemmeringen voor het vrije verkeer van goederen en diensten geconstateerd die als gerechtvaardigd kunnen worden beschouwd om redenen van algemeen belang*, en derhalve geacht kunnen worden verenigbaar te zijn met de beginselen van het Verdrag. Met betrekking tot deze belemmeringen *kan een communautaire maatregel om de werking van de interne markt zeker te stellen noodzakelijk blijken*.

---

26 Bijvoorbeeld de Britse regelgeving.

27 Bijvoorbeeld de Ierse regelgeving.

28 Arrest "Mediawet" van 25.07.1991, zaak 288/89, jurispr. 1991, blz. I-4007.

1. De belemmeringen voor het vrije verkeer van decodeeruitrustingen (artikelen 30 en volgende van het Verdrag)

Artikel 30 bepaalt dat kwantitatieve invoerbeperkingen en alle maatregelen van gelijke werking tussen de Lid-Staten verboden zijn[29]. Regelingen die een *verbod inhouden op de vervaardiging en het in de handel brengen* van illegale uitrustingen zijn *zonder onderscheid van toepassing*[30] en hebben *beperkende gevolgen* voor het handelsverkeer, voor zover hierdoor belemmeringen ontstaan voor de invoer en het in de handel brengen van uit andere Lid-Staten afkomstige produkten.

Overeenkomstig de jurisprudentie van het Hof zijn deze verbodsbepalingen gerechtvaardigd, omdat hiermee doelstellingen van algemeen belang worden nagestreefd. Zij zijn gericht op de *bescherming van de encrypterende organisatie tegen diegenen die*

---

29 In dit verband dient te worden opgemerkt dat het Hof traditioneel kwantitatieve beperkingen definieert als invoerverbod of invoerbeperkingen, en maatregelen van gelijke werking als "iedere handelsregeling der Lid-Staten die de intracommunautaire handel al dan niet rechtstreeks, daadwerkelijk of potentieel, kan beïnvloeden" (arrest "Dassonville" van 11.7.1974, zaak 8/74, jurispr. 1974, blz. 837).

Binnen deze laatste categorie brengt het Hof evenwel een onderscheid aan. Enderzijds acht het de handelsregelingen die maatregelen van gelijke werking als kwantitatieve beperkingen vormen onverenigbaar met artikel 30, aangezien deze voorwaarden opleggen die uitsluitend gelden voor ingevoerde produkten, of de verkoop of het gebruik daarvan moeilijker of duurder maken dan van nationale produkten (maatregelen die niet zonder onderscheid van toepassing zijn). Deze maatregelen kunnen, evenals kwantitatieve beperkingen, voor zover deze discriminerend zijn, slechts worden gerechtvaardigd op de in artikel 36 genoemde gronden.

Wat anderzijds de nationale regelingen betreft die identieke gevolgen hebben voor ingevoerde en nationale produkten, heeft het Hof verklaard dat, zelfs indien deze zonder onderscheid van toepassing zijn op nationale en ingevoerde produkten (maatregelen die zonder onderscheid van toepassing zijn), deze regelingen slechts belemmeringen kunnen vormen voor een produkt dat op wettige wijze is vervaardigd en/of in het verkeer is gebracht in een andere Lid-Staat, voor zover dringende behoeften ze noodzakelijk maken (waartoe het Hof, naast de in artikel 36 genoemde redenen van algemeen belang, de bescherming van de volksgezondheid of het milieu, de eerlijkheid van de handelstransacties, enzovoorts, rekent) (arresten "Cassis de Dijon" van 20.02.1979, zaak 120/78, jurispr. 1979, blz. 649, en "Commissie/Frankrijk" van 23.02.1988, zaak 216/84, jurispr. 1988, blz. 793).

In dit geval zijn de belemmeringen voor het vrije verkeer van goederen die voortvloeien uit de verschillen tussen de nationale regelingen gerechtvaardigd, indien er een rechtstreeks verband bestaat tussen de regeling en de dringende behoefte (causaliteitscriterium), deze passend is en niet buiten verhouding staat tot de beoogde behoefte (proportionaliteitscriterium), er in het land van oorsprong geen gelijkwaardige wetgeving is, en er geen alternatieve oplossingen bestaan waarmee het nagestreefde doel bereikt kan worden en de handelsstromen in mindere mate verstoord worden (substitutiecriterium).

Derhalve kan een nationale regeling, hoewel deze zonder onderscheid van toepassing is, toch neerkomen op een maatregel van gelijke werking, wanneer de beperkende gevolgen daarvan voor het handelsverkeer binnen de Gemeenschap weliswaar gerechtvaardigd worden door een dringende behoefte, maar verder gaan dan hetgeen noodzakelijk is om het nagestreefde doel te bereiken.

30 Zij hebben niet tot gevolg dat de nationale produkten worden bevoordeeld, maar leiden tot dezelfde beperkingen voor zowel nationale als ingevoerde produkten.

op frauduleuze wijze profiteren van haar activiteiten (de fabrikanten en distributeurs van niet-erkende decodeeruitrustingen), en op de *bescherming van de consument* tegen het in omloop brengen van uitrustingen die de ontvangst van de dienst niet langer mogelijk maken wanneer de exploitant van systeem verandert, omdat zij niet officieel zijn. Een dergelijke doelstelling van economische betrekkingen die hun beslag krijgen in een billijke en eerlijke omgeving, behoort tot de redenen van algemeen belang die volgens het Hof gerechtvaardigde beperkingen zijn van het vrije verkeer van goederen[31].

Bovendien wordt met deze verbodsbepalingen beoogd het recht op een vergoeding te beschermen van de houders van *intellectuele eigendomsrechten* op de geëncrypteerde uitzendingen en van de houders van *industriële en intellectuele eigendomsrechten* die op de uitrustingen rusten[32]. Het aldus gewaarborgde recht op een legitieme vergoeding van zowel de rechthebbenden op de programma's als de rechthebbenden op de technologie die de illegale uitrustingen bevatten, behoort tot de rechten die, in de bewoordingen van het Hof, het specifiek voorwerp van de *industriële en intellectuele eigendom* vormen[33].

De betrokken regelingen voldoen ook aan het *proportionaliteitscriterium*, aangezien zij zich beperken tot het verbieden van het in het verkeer brengen van uitrustingen die vervaardigd zijn zonder voorafgaande toestemming van de encrypterende organisatie, ongeacht of deze uitrustingen uit het eigen land of het buitenland afkomstig zijn. Zij gaan dus niet verder dan hetgeen noodzakelijk is om de nagestreefde doelstelling te bereiken[34]. Ten slotte voldoen deze regelingen eveneens aan de *substitutie- en equivalentiecriteria*, aangezien er geen alternatieve en minder beperkende maatregelen voorhanden zijn om de nagestreefde bescherming te waarborgen.

Concluderend kan een beperking van het vrije verkeer van decodeeruitrustingen die in de Lid-Staat van oorsprong zonder voorafgaande toestemming zijn vervaardigd en in het verkeer zijn gebracht, gerechtvaardigd zijn uit hoofde van de bescherming van de consument, de eerlijkheid van de handelstransacties en de intellectuele en industriële eigendom.

---

31 Arresten "Bequelin" van 25.11.1971, zaak 22/71, jurispr. 1971, blz. 970, en "Dansk Supermarked" van 22.01.1981, zaak 58/80, jurispr. 1981, blz. 181.

32 Om deze reden verwijst een aantal nationale bepalingen naar de auteurswetgeving. Hierbij wordt aan de belanghebbende partijen (doorgaans de encrypterende organisatie) dezelfde rechten toegekend als de rechthebbenden op een beschermd werk hebben met betrekking tot kopieën die zonder toestemming van het werk zelf zijn vervaardigd. In beide gevallen berooft de zonder goedkeuring vervaardigde kopie, of het daarbij nu gaat om een werk of om een decodeeruitrusting die de ontvangst van een dienst mogelijk maakt, de rechthebbende of de dienstverrichter van zijn legitieme vergoeding.

33 Arrest "Deutsche Grammophon" van 08.06.1971, zaak 78/70, jurispr. 1971, blz. 502.

34 De toepassing van de betrokken verbodsbepalingen op de invoer en het in de handel brengen van uitrustingen die in de Lid-Staat van oorsprong zijn vervaardigd en in de handel gebracht *met toestemming van de encrypterende organisatie*, kan echer leiden tot economische beperkingen die buiten verhouding staan tot het nagestreefde doel en derhalve onverenigbaar zijn met de beginselen inzake het vrije verkeer van goederen als uitgelegd door het Hof.

2. De belemmeringen voor het vrij verrichten van diensten die verband houden met decodeeruitrustingen (artikelen 59 en volgende)

De analyse van de nationale regelingen heeft aangetoond dat bepaalde landen de activiteiten verbieden die verband houden met de vervaardiging en het in het verkeer brengen van illegale decodeeruitrustingen, zoals *het maken van reclame voor en het installeren, onderhouden en vervangen van illegale decodeeruitrustingen*.

Deze activiteiten vormen dienstverrichtingen in de zin van de artikelen 59 en 60 van het Verdrag. Hoewel de betrokken verbodsbepalingen zonder onderscheid van toepassing zijn, hebben zij beperkende gevolgen voor het vrij verrichten van diensten. Reclame-activiteiten en/of service na de verkoop door in andere Lid-Staten gevestigde dienstverrichters worden immers verboden.

Volgens de jurisprudentie van het Hof[35] kunnen deze beperkingen gerechtvaardigd zijn, indien met de betrokken regelingen doelstellingen van algemeen belang als de *bescherming van de consument*[36] en de *industriële en intellectuele eigendom*[37] worden nagestreefd. Bovendien gaan deze beperkende gevolgen niet verder dan hetgeen noodzakelijk is om het nagestreefde doel te bereiken en kunnen derhalve geacht worden proportioneel te zijn[38].

Concluderend kan een verbod op het maken van reclame voor en het installeren, onderhouden en vervangen van uitrustingen die in de Lid-Staat van oorsprong zonder voorafgaande toestemming van de encrypterende organisatie zijn vervaardigd en in het

---

35 Het HvJEG heeft een onderscheid gemaakt tussen beperkingen die discriminerend zijn en beperkingen die zonder onderscheid van toepassing zijn. De eerstgenoemde beperkingen kunnen gerechtvaardigd zijn op een der in artikel 56 genoemde gronden (openbare orde, openbare veiligheid en volksgezondheid). Met betrekking tot maatregelen die leiden tot beperkingen die zonder onderscheid gelden, heeft het Hof echter verklaard dat artikel 59 niet alleen de afschaffing van iedere discriminatie tegen een dienstverrichter op grond van diens nationaliteit verlangt, maar tevens "de opheffing van ieder beperking - ook indien deze zonder onderscheid geldt voor binnenlandse dienstverrichters en dienstverrichters uit andere Lid-Staten - die de werkzaamheden van de dienstverrichter die in een andere Lid-Staat is gevestigd en aldaar rechtmatig soortgelijke diensten verricht, verbiedt of anderszins belemmert" (arrest "Dennemeyer", 25.07/1991, zaak 76/90, jurispr. 1991). Hieruit vloeit volgens het Hof voort dat een verbod dat zonder onderscheid geldt het vrij verrichten van diensten slechts kan beperken, voor zover deze beperkingen gerechtvaardigd worden door dwingende redenen van algemeen belang, dit belang niet wordt gewaarborgd door de regels van de Lid-Staat waar de dienstverrichter is gevestigd, en hetzelfde resultaat niet met minder beperkende regels kan worden bereikt. Tot dwingende redenen van algemeen belang rekent het Hof de bescherming van consumenten en werknemers, de industriële en commerciële eigendom, enzovoorts.

36 Arrest "Commissie/Frankrijk" van 4.12.1986, zaak 220/83, jurispr. 1986, blz. 3663.

37 Arrest "Coditel" van 18.03.1980, zaak 62/79, jurispr. 1980, blz. 881.

38 De uitkomst zou waarschijnlijk anders zijn in het geval van uitrustingen die in de Lid-Staat van oorsprong zijn vervaardigd en in het verkeer gebracht *met toestemming van de encrypterende organisatie*. In dit geval leiden deze beperkende maatregelen tot belemmeringen van de handelsbetrekkingen tussen de Lid-Staten die buiten verhouding staan tot het nagestreefde doel en derhalve onverenigbaar zijn met de beginselen van het Verdrag inzake het vrij verrichten van diensten als uitgelegd door het Hof.

verkeer gebracht, gerechtvaardigd zijn uit hoofde van de bescherming van de consument en van de industriële en intellectuele eigendom.

3. De belemmeringen voor het vrij verrichten van geëncrypteerde diensten

De belemmeringen voor het vrij verrichten van geëncrypteerde diensten kunnen bovendien het gevolg zijn van het *ontbreken van rechtsbescherming in bepaalde Lid-Staten van ontvangst*. Zoals bevestigd werd door de raadpleging van de Commissie, is een doelmatige rechtsbescherming tegen illegale ontvangst voor de exploitanten een belangrijk element in de besluitvorming over het al dan niet distribueren van de dienst in een bepaald land. Het ontbreken van een dergelijke rechtsbescherming *maakt de introductie ongetwijfeld moeilijker en riskanter*. De exploitanten zien zich gesteld tegenover extra kosten, die niet alleen het gevolg zijn van het gebruik van een extra veilig systeem, maar ook van de noodzaak om de distributie van de decodeeruitrustingen aan te passen (doorgaans middels verhuur), hetgeen zeer duur kan zijn.

Een dergelijk juridisch vacuüm heeft derhalve *beperkende gevolgen* voor het verkeer van geëncrypteerde diensten binnen de interne markt, omdat de distributie daarvan bemoeilijkt wordt in landen waar geen rechtsbescherming tegen illegale ontvangst bestaat.

Deze beperkende gevolgen zijn echter niet in strijd met het gemeenschapsrecht, omdat, zoals door het Hof is erkend[39], de Lid-Staten vrij zijn om bij gebreke van harmonisatie op gemeenschapsniveau regels vast te stellen voor de economische activiteiten op hun grondgebied, in overeenstemming met de beginselen van het Verdrag. Zij kunnen derhalve, met inachtneming van het proportionaliteitsbeginsel, besluiten om bepaalde activiteiten al dan niet te verbieden om redenen van algemeen belang.

Concluderend kan het regelgevingsbeleid ten aanzien van de economische activiteiten, dat elke Lid-Staat bij gebreke van harmonisatie op gemeenschapsniveau naar eigen inzicht kan voeren, een rechtvaardiging vormen voor de lacunes in de wetgeving.

4. Vervalsing van de mededinging

De verschillen tussen de nationale regelingen en het ontbreken van dergelijke regelingen in bepaalde Lid-Staten kunnen bovendien *vervalsing van de mededinging* binnen de interne markt in de hand werken. Een exploitant die zijn decodeeruitrustingen distribueert in een Lid-Staat waar een goede rechtsbescherming bestaat, geniet concurrentievoordelen (die weer invloed hebben op bijvoorbeeld zijn vermogen om programma's aan te kopen) ten opzichte van een exploitant die zijn dienst distribueert in een Lid-Staat waar geen doelmatige rechtsbescherming voorhanden is, omdat deze laatste de aanvullende kosten moet dragen van bijvoorbeeld een extra veilig distributiesysteem.

Deze verschillen in mededingingsvoorwaarden in de Lid-Staten kunnen negatieve gevolgen hebben voor de ontwikkeling van geëncrypteerde diensten op de interne markt, aangezien de exploitanten binnen de Europese Unie niet onder dezelfde marktvoorwaarden actief zijn.

---

[39] Arrest "Procureur des Konings/Debauve" van 18.03.1980, zaak 52/79, jurispr. 1980, blz. 833.

Concluderend kunnen de verschillen tussen de nationale regelingen leiden tot vervalsing van de mededinging, waardoor de ontwikkeling van geëncrypteerde diensten kan worden bemoeilijkt.

Vraag 2 : De Commissie zou kennis willen nemen van de mening van de belanghebbende partijen over het bestaan van andere beperkingen en beperkende gevolgen dan die, welke in het voorgaande zijn beschreven.

HOOFDSTUK 5 : NOODZAAK VAN EEN COMMUNAUTAIR INITIATIEF EN MOGELIJKE MAATREGELEN

Uit de voorgaande analyse is gebleken dat er nog immer een aantal *belemmeringen voor de werking van de interne markt* bestaan. Bepaalde daarvan zijn mogelijk *onverenigbaar met het gemeenschapsrecht* en moeten derhalve worden opgeheven. Dit geldt voor de belemmeringen die ontstaan door de toepassing van nationale regelingen waarbij met het oog op de rechtsbescherming van geëncrypteerde diensten onderscheid wordt gemaakt naar *aard* (via de ether of per satelliet) of *herkomst van de dienst*.

Andere belemmeringen kunnen evenwel *gerechtvaardigd zijn om redenen van algemeen belang, zoals de bescherming van de consument en de industriële en intellectuele eigendom, en in het licht van het proportionaliteitsbeginsel*. Dit geldt ten eerste voor de belemmeringen van het vrije verkeer van decodeeruitrustingen en daarmee verbonden diensten, welke het gevolg zijn van de verschillen tussen de nationale regelingen inzake het vervaardigen en in het verkeer brengen van decodeeruitrustingen.

Bovendien is uit de raadpleging gebleken dat de huidige fragmentatie van de regelgeving in economisch opzicht, met de extra kosten en de rechtsonzekerheid die daaruit voortvloeien, door de betrokken beroepskringen gezien wordt als een *aanzienlijke belemmering voor de ontwikkeling van nieuwe geëncrypteerde diensten*. Een doelmatige rechtsbescherming tegen illegale ontvangst kan een investeerder ertoe bewegen een nieuwe dienst te ontwikkelen of in andere Lid-Staten op de markt te brengen.

Wat deze laatste belemmeringen betreft, *kan een maatregel, welke erop gericht is een gelijkwaardig beschermingsniveau in alle Lid-Staten tot stand te brengen, noodzakelijk blijken om deze belemmeringen weg te nemen en om het regelgevingskader voor de Europese audiovisuele sector aan te vullen dat tot stand is gebracht door de richtlijnen "Televisie zonder grenzen" (89/552/EEG) en "Kabel en satelliet" (93/83/EEG).*

In dit opzicht moet worden benadrukt dat de doelstelling van de afschaffing van de belemmeringen voor de goede werking van de interne markt, welke het gevolg zijn van de verschillen tussen de nationale regelingen inzake de juridische bescherming van geëncrypteerde diensten, slechts kan worden verwezenlijkt door middel van *communautaire harmonisatie*. Het lijkt namelijk weinig waarschijnlijk dat de Lid-Staten spontaan zouden overgaan tot een onderlinge toenadering van de nationale regelingen op het gebied van de rechtsbescherming van geëncrypteerde diensten. Zelfs indien dit wel het geval zou zijn, zou deze toenadering bij gebreke van een institutioneel kader in de communautaire rechtsorde weinig efficiënt zijn en de industrie niet de voor het ontwikkelen van geëncrypteerde diensten noodzakelijke rechtszekerheid bieden.

Alvorens tot een wetgevingsinitiatief te besluiten, zou de Commissie kennis willen nemen van de mening van de belanghebbende partijen over de in het navolgende uiteengezette opties.

1. Doel van de maatregel

Het algemene doel van de maatregel zou zijn de mediasectoren (zowel de verrichters van geëncrypteerde diensten als de leveranciers van programma's en de fabrikanten van de

uitrustingen) in staat te stellen ten volle de mogelijkheden te benutten die de interne markt biedt. Met name met het oog op de informatiemaatschappij bestaat het gevaar dat deze mogelijkheden niet volledig worden benut, indien de ondernemingen binnen de Unie niet beschikken over een toereikende rechtsbescherming.

Een duidelijk regelgevingskader, dat in de gehele Gemeenschap *rechtsbescherming* biedt tegen illegale ontvangst en aldus het *vrije verkeer* van deze diensten en goederen waarborgt, is een onmisbare voorwaarde voor de ontwikkeling van nieuwe diensten.

Aangezien het probleem van de illegale ontvangst zich wereldwijd voordoet, dienen ook initiatieven op internationaal niveau te worden genomen, met name in het kader van bilaterale overeenkomsten en van de WTO, om effectieve regels op mondiaal niveau vast te stellen. Een maatregel om een regelgevingskader voor de interne markt tot stand te brengen, zou onvolledig zijn indien deze niet vergezeld zou gaan van een vergelijkbare externe maatregel, welke gericht is op de oplossing van het probleem op het internationale vlak en *bescherming biedt tegen invoer uit derde landen.*

2. Samenhang met ander communautair beleid

Een wetgevingsinitiatief om de rechtsbescherming van geëncrypteerde diensten te waarborgen, zou bovendien stroken met *andere communautaire doelstellingen en beleidsgebieden*.

- *Een regelgevingskader dat een hoog beschermingsniveau biedt op unieniveau zou bijdragen tot de ontwikkeling van de Europese industrie van geëncrypteerde diensten en decodeeruitrustingen*. Indien een doelmatige rechtsbescherming ontbreekt, kunnen de illegale ontvangst en de winstderving die daarvan het gevolg is de financiële stabiliteit van de verrichters van geëncrypteerde diensten ondermijnen en de ontwikkeling van deze diensten bemoeilijken. Soortgelijke gevolgen zullen de fabrikanten van decodeeruitrustingen ondervinden, die zich zonder rechtsbescherming niet zullen toeleggen op een activiteit die niet beschermd is tegen frauduleuze handelingen;

- *Een wettelijke maatregel om de goede werking van de interne markt te waarborgen zou stroken met de doelstellingen van het audiovisueel beleid en het cultuurbeleid van de Unie*. Een dergelijke maatregel zou een betere exploitatie van de intellectuele eigendomsrechten op de door de zenders uitgezonden programma's mogelijk maken, waardoor de exploitatiemogelijkheden voor de *audiovisuele sector* toenemen. De nieuwe geëncrypteerde diensten vormen een sterke impuls voor de ontwikkeling en het verkeer van artistieke creaties en voor de ontplooiing van de culturele en taaldiversiteit van de Unie. De houders van de rechten zullen evenwel niet geneigd zijn om deze over te dragen, indien de geëncrypteerde diensten niet beschermd zijn tegen illegale ontvangst. In een dergelijke situatie kunnen de geëncrypteerde diensten zich bij gebrek aan programma's niet ontwikkelen en verliest de audiovisuele sector de voordelen van een doeltreffende verspreidingsmethode.

- *Een wettelijke maatregel om de werking van de interne markt te waarborgen zou stroken met de doelstelling van de bescherming van de consument*. Indien zekerheid biedende regels ontbreken, kunnen consumenten op het moment van aankoop misleid worden met betrekking tot de herkomst van de decodeeruitrusting en geloven dat zij een erkende uitrusting kopen, terwijl het in werkelijkheid een illegale uitrusting is. Wanneer de exploitant in dit geval om veiligheidsredenen het encryptiesysteem moet wijzigen, is de gekochte uitrusting van geen enkel nut meer voor de consument, die op eigen kosten een andere decoder zal moeten kopen. Anderzijds rust op niet-erkende uitrustingen soms geen garantie, zodat de consument bij een slechte werking ook de reparatiekosten zelf zal moeten dragen. In beide gevallen zijn de negatieve gevolgen voor de consument van de aanwezigheid op de markt van niet-erkende uitrustingen evident. Bovendien hebben de verliezen die de dienstverrichters ondervinden negatieve gevolgen voor hun financiële stabiliteit, waardoor de ontwikkeling van geëncrypteerde diensten vertraagd wordt. Deze situatie, die ontstaat door het ontbreken van bescherming, betekent ook een verlies voor de consument, die de dienst niet langer kan genieten.

3. Keuze van rechtsinstrument en rechtsbasis

Op basis van de voorgaande analyse kan de Commissie na raadpleging van de belanghebbende partijen een van de twee volgende beslissingen nemen.

De Commissie zou een *richtlijn voor de harmonisering van de nationale regelingen* kunnen voorstellen (optie 1). Rekening houdend met de beginselen van proportionaliteit en subsidiariteit, zou de voorgestelde richtlijn een minimum-harmonisatie kunnen behelzen, waarbij het de Lid-Staten vrij staat om zelf stringentere beginselen vast te stellen, maar tevens een gelijkwaardig *minimum-beschermingsniveau* binnen de Unie wordt geboden. Deze optie zou het voordeel hebben dat de belanghebbende kringen rechtszekerheid wordt geboden, terwijl de Lid-Staten een zekere flexibiliteit behouden met betrekking tot de uitbreiding van deze bescherming.

De Commissie zou anderzijds een *verordening van de Raad* kunnen voorstellen (optie 2). Deze optie zou dezelfde doelstellingen hebben als de eerste optie, maar de harmonisatie zou doelmatiger zijn, omdat de verordening rechtstreeks in de Lid-Staten van toepassing is en niet in nationaal recht behoeft te worden omgezet.

De gekozen optie zou vergezeld kunnen worden van een voorstel tot wijziging van de bestaande communautaire regelgeving op het gebied van het in het vrije verkeer brengen van nagemaakte goederen uit derde landen[40], zodat deze ook van toepassing is op decodeeruitrustingen. Hierbij dient echter te worden aangetekend dat deze wijziging op zich niet voldoende zou zijn om een doelmatige rechtsbescherming binnen de Unie te waarborgen. De bepalingen van de verordening inzake nagemaakte goederen zijn slechts

---

40 Verordening (EG) nr. 3295/94 van de Raad (PB nr. L 341 van 30.12.1994) tot vaststelling van maatregelen om het in het vrije verkeer brengen, de uitvoer, de wederuitvoer en de plaatsing onder een schorsingsregeling van nagemaakte of door piraterij verkregen goederen te verbieden.

op vrijwillige basis van toepassing voor de betrokken exploitanten of ondernemingen, en dan alleen op goederen die uit derde landen afkomstig zijn, en op het moment van invoer in de Unie. Op het handelsverkeer tussen de Lid-Staten zijn de nationale en communautaire regelingen van toepassing. Op het gebied van de vervaardiging en het in de handel brengen van illegale decodeeruitrustingen bestaat momenteel geen uniforme nationale regelgeving, waardoor de mogelijke oplossingen uiteenlopen en bescherming in bepaalde gevallen ontbreekt. Een maatregel om de controle op de invoer uit derde landen te waarborgen, zou derhalve noodzakelijkerwijs gepaard dienen te gaan met een wetgevingsvoorstel waarbij de bescherming tegen illegale ontvangst binnen de Unie gewaarborgd wordt.

De geëigende rechtsbasis zou gevormd worden door de artikelen 57, lid 2, 66 en 100a, omdat beoogd wordt de goede werking van de interne markt zeker te stellen en het vrije verkeer van goederen en diensten mogelijk te maken[41].

4. Toepassingsgebied

De beoogde harmonisatie heeft betrekking op de *bestaande nationale regelingen op het gebied van de rechtsbescherming van geëncrypteerde diensten*. Deze regelingen, voor zover zij bestaan, kunnen deel uitmaken van het auteursrecht, het omroeprecht, het privaatrecht of het administratiefrecht. De plaats van deze regelingen is echter zonder belang; wat telt is de doelstelling, namelijk de bescherming van geëncrypteerde diensten tegen illegale ontvangst.

Deze harmonisatie kan betrekking hebben op *alle geëncrypteerde diensten*, waarbij *gebruik wordt gemaakt van encryptie om de betaling van een vergoeding zeker te stellen*, en hoeft zich niet te beperken tot omroepdiensten. Tot deze categorie behoren derhalve de *traditionele geëncrypteerde omroepdiensten* (via de kabel, de ether of per satelliet), de *nieuwe omroepdiensten* (digitale televisie, *pay-per-view*, *near-video-on-demand*), en *diensten van de informatiemaatschappij, met andere woorden, diensten die elektronisch op afstand op individuele aanvraag van de ontvanger worden geleverd* (video op aanvraag, spelletjes op verzoek, interactief telewinkelen).

Derhalve dienen *alle geëncrypteerde diensten*, waarvoor decodeeruitrustingen verkrijgbaar zijn voor het publiek, *in aanmerking te komen voor dezelfde bescherming*. In het vooruitzicht van de convergentie van omroepdiensten en informaticadiensten dient de definitie van "geëncrypteerde diensten" elke dienst te omvatten die kan worden ontvangen op een televisie- of computerscherm, dus de radio- en televisie-omroepdiensten en de andere, interactieve diensten van de informatiemaatschappij, zoals gedefinieerd in het voorstel voor een richtlijn inzake de doorzichtigheid van de regelgeving voor de interne markt, ofwel de diensten op afstand die elektronisch worden geleverd op aanvraag van de ontvanger van de dienst.

Deze harmonisatie zou daarentegen *geen betrekking dienen te hebben* op diensten waarbij encryptie wordt gebruikt voor andere doeleinden dan het waarborgen van de betaling van een vergoeding, zoals het geval is bij diensten die geëncrypteerd worden om *de integriteit*

---

41 Indien gedacht wordt aan een wijziging van de verordening inzake nagemaakte produkten, blijft de rechtsbasis onverminderd artikel 113.

en vertrouwelijkheid van de boodschap veilig te stellen, namelijk financiële diensten en telecommunicatiediensten. De reden hiervoor is dat bij deze laatste diensten het *algemeen belang* dat bij onderschepping wordt geschaad, te weten de integriteit en vertrouwelijkheid van de boodschap, wezenlijk verschilt van de bescherming van de waarde van een dienst die tegen betaling wordt verricht als doelstelling van algemeen belang die bedreigd wordt door de illegale ontvangst. Dit verschil heeft op nationaal en internationaal niveau geleid tot *sterk uiteenlopende regelingen*, met name wat betreft de maatregelen en de strafmaat, die een gemeenschappelijke aanpak van de beide problemen niet rechtvaardigen.

De bescherming tegen goederen die afkomstig zijn uit derde landen, zou moeten gelden voor alle decodeeruitrustingen die uit een derde land zijn ingevoerd en waarmee een geëncrypteerde dienst kan worden ontvangen zonder voorafgaande toestemming van de encrypterende organisatie.

5. Algemene structuur

Rekening houdend met het proportionaliteitsbeginsel, zouden de beoogde bepalingen de volgende activiteiten kunnen verbieden :

- De vervaardiging van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- De verkoop van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- Het bezit voor commerciële doeleinden van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- Het bezit voor privédoeleinden van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- De installatie, het onderhoud en de vervanging van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- Het maken van reclame voor decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie;

- Het decoderen van geëncrypteerde uitzendingen zonder toestemming van de encrypterende organisatie.

De voorgestelde maatregel dient ook te bepalen dat de Lid-Staten *doelmatige, evenredige en ontmoedigende sancties op inbreuken vaststellen*. In dit opzicht blijven de Lid-Staten, zoals de Commissie heeft opgemerkt in de mededeling betreffende de rol van sancties voor de tenuitvoerlegging van de communautaire wetgeving[42], vrij om het sanctieregime vast te stellen. De maatregel zou overigens een kennisgevingsprocedure kunnen bevatten voor de bepalingen die de Lid-Staten in dit opzicht hebben vastgesteld.

Bovendien zou elke belanghebbende partij de mogelijkheid geboden moeten worden een *rechtsvordering tot vergoeding van schade en intresten* in te stellen.

Wat de bepalingen inzake de bescherming tegen het in het verkeer brengen van uit derde landen afkomstige goederen betreft, zou de maatregel een verbod dienen te bevatten op de invoer van decodeeruitrustingen die bestemd zijn om de toegang tot geëncrypteerde diensten mogelijk te maken zonder toestemming van de encrypterende organisatie.

Vraag 3 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de behoefte aan harmonisatie op communautair niveau.

Vraag 4 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de vraag, welke van de in het groenboek beschreven opties zou moeten worden gekozen om vorm te geven aan een eventueel harmonisatie-instrument.

Vraag 5 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de inhoud van een eventueel harmonisatie-instrument als in het voorgaande omschreven, met name wat betreft :

i. ***het toepassingsgebied :***
   - *a.* ***dient deze beperkt te blijven tot omroepdiensten of uitgebreid te worden tot alle diensten die geëncrypteerd worden om de betaling van een vergoeding zeker te stellen;***
   - *b.* ***indien de voorkeur gegeven wordt aan de uitbreiding, is het gekozen criterium (geëncrypteerde diensten om de betaling van een vergoeding zeker te stellen) geschikt, of moet een ander criterium worden gekozen om het toepassingsgebied af te bakenen? Zo ja, bent u van mening dat het harmonisatie-instrument bescherming tegen illegale ontvangst zou moeten bieden voor alle diensten, geëncrypteerd of niet, waarbij gebruik gemaakt wordt van technieken voor voorwaardelijke toegang, met inbegrip van bij voorbeeld passwords?***

ii. ***het al dan niet opnemen van het bezit door particulieren van niet-erkende uitrustingen;***

iii. ***vorderingen tot vergoeding van schade en intresten.***

---

42 "Mededeling van de Commissie aan de Raad en het Europees Parlement betreffende de rol van sancties voor de tenuitvoerlegging van de communautaire wetgeving op het gebied van de interne markt", COM(95) 162 def. van 03.05.1995.

VRAGENLIJST

Vraag 1 : De Commissie zou gaarne aanvullende gegevens ontvangen om een uitvoeriger analyse van de vastgestelde nationale regelgeving te kunnen maken.

Vraag 2 : De Commissie zou kennis willen nemen van de mening van de belanghebbende partijen over het bestaan van andere beperkingen en beperkende gevolgen dan die, welke in het voorgaande zijn beschreven.

Vraag 3 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de behoefte aan harmonisatie op communautair niveau.

Vraag 4 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de vraag, welke van de in het groenboek beschreven opties zou moeten worden gekozen om vorm te geven aan een eventueel harmonisatie-instrument.

Vraag 5 : De Commissie zou de mening van de belanghebbende partijen willen vernemen over de inhoud van een eventueel harmonisatie-instrument als in het voorgaande omschreven, met name wat betreft :

i. ***het toepassingsgebied :***

- *a.* ***dient deze beperkt te blijven tot omroepdiensten of uitgebreid te worden tot alle diensten die geëncrypteerd worden om de betaling van een vergoeding zeker te stellen?;***
- *b.* ***indien de voorkeur gegeven wordt aan de uitbreiding, is het gekozen criterium (geëncrypteerde diensten om de betaling van een vergoeding zeker te stellen) geschikt, of moet een ander criterium worden gekozen om het toepassingsgebied af te bakenen? Zo ja, bent u van mening dat het harmonisatie-instrument bescherming tegen illegale ontvangst zou moeten bieden voor alle diensten, geëncrypteerd of niet, waarbij gebruik gemaakt wordt van technieken voor voorwaardelijke toegang, met inbegrip van bij voorbeeld passwords?***

ii. ***het al dan niet opnemen van het bezit door particulieren van niet-erkende uitrustingen;***

iii. ***vorderingen tot vergoeding van schade en intresten.***

ISSN 0254-1513

COM(96) 76 def.

DOCUMENTEN

NL 15 10

Catalogusnummer : CB-CO-96-102-NL-C

ISBN 92-78-01338-2

Bureau voor officiële publikaties der Europese Gemeenschappen

L-2985 Luxemburg