KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 24.04.2003
KOM(2003) 198 endelig

OM RETLIG BESKYTTELSE AF ELEKTRONISKE BETALINGSTJENESTER

Rapport fra Kommissionen til Rådet, Europa-Parlamentet og Det Europæiske Økonomiske og Sociale Udvalg

om gennemførelsen af Europa-Parlamentets og Rådets direktiv 98/84/EF af 20. november 1998 om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester

Resumé

Denne første rapport fra Kommissionen om gennemførelsen af direktiv 98/84/EF, der sigter mod at tilvejebringe et minimumsniveau af **retlig beskyttelse inden for EU af elektroniske betalingstjenester** (betalingstv-, -radio- og -internettjenester) **mod piratvirksomhed,** er et led i Kommissionens omfattende strategi for det indre marked for at fjerne hindringer for handel med tjenesteydelser. Den indeholder en beskrivelse og gennemgang af de væsentligste fakta om direktivets vigtigste bestemmelser, en redegørelse for, hvordan de er gennemført og håndhæves i medlemsstater og kandidatlande, og kortlægger aktuelle tendenser inden for piratvirksomhed. Den dækker perioden mellem direktivets vedtagelse i november 1998 og indtil udgangen af 2002.

Det konkluderes i rapporten, at det 21. århundredes videnbaserede økonomier i stadigt stigende grad ventes at bygge på **påtrængende elektroniske betalingstjenester**, og at piratvirksomhed vil have samme skadelige virkning på vidensamfundet som økonomisk kriminalitet og vareforfalskning i det 20. århundrede. Den retlige beskyttelse mod piratvirksomhed over for elektroniske betalingstjenester vil være et vigtigt **bidrag til at nå EU's ambitiøse mål om at blive den mest dynamiske og konkurrencedygtige økonomi i verden senest i 2010**.

I rapporten fremhæves den piratvirksomhed, der er en følge af, at det er umuligt at få adgang til **beskyttede satellittv-kanaler fra andre medlemsstater**. Det konstateres endvidere, at EU's borgere har vanskeligt ved at forstå, hvorfor de inden for det indre marked ikke kan få lovlig adgang til beskyttede betalingstv-tjenester, selv om de er villige til at betale for det. I rapporten opfordres aktørerne på markedet derfor til aktivt at søge **aftalebaserede løsninger,** og det fremgår, at Kommissionen vil bidrage til denne proces, når den gennemgår direktivet om ophavsret, for så vidt angår radio- og tv-udsendelse via satellit og viderespredning pr. kabel.

Rapporten viser, at **gennemførelsen** af direktivet endnu ikke er helt på plads inden for det udvidede EU, at **håndhævelsen** på nationalt plan skal konsolideres, og at en **fælles indsats** er afgørende for en effektiv bekæmpelse af piratvirksomhed. Det er kun muligt at bekæmpe piratvirksomhed, hvis pirater ikke kan finde noget fristed i Europa. Kommissionen vil derfor fortsætte sit samarbejde med andre europæiske lande og relevante internationale organisationer for at skabe **en sammenhængende, tværeuropæisk retlig ramme mod piratvirksomhed over for elektroniske betalingstjenester**, særlig ved at sikre en hurtig ikrafttrædelse af Europarådets konvention nr. 178.

Det hedder i rapporten, at **piratvirksomhed mod elektroniske betalingstjenester betragtes som cyberkriminalitet**. Det konkluderes, at det er for **tidligt at foreslå ændringer** af direktivet, men at høringerne og vurderingerne, som er gennemført i forbindelse med rapporten, har givet Kommissionen mulighed for allerede nu at afdække en række problemstillinger, som fortjener nærmere overvejelse i tæt samarbejde med medlemsstaterne og erhvervslivet. Det gælder bl.a. behovet for **afbalancerede og sammenhængende rammer for håndhævelsen**, som kan anvendes på alle former for piratvirksomhed og varemærkeforfalskning, og som der er enighed om på fællesskabsplan, samt på **distribution af nøgler og ulovlige anordninger** via internet.

INDHOLDSFORTEGNELSE

1. INDLEDNING

Dette dokument indeholder Kommissionens første rapport til Europa-Parlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg om gennemførelsen af direktiv 98/84/EF[1] om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester (herefter benævnt "direktivet").

Direktivet sigter mod at tilvejebringe et minimumsniveau i EU for retlig beskyttelse af elektroniske betalingstjenester mod piratvirksomhed ved at forbyde al kommerciel fremstilling, distribution og markedsføring af piratkopierede smart cards og andre anordninger, der omgår adgangsstyringen hos betalingstv-, -radio- og -internettjenester.

Det er fastsat i direktivets artikel 7, at Kommissionen senest tre år efter direktivets ikrafttræden[2] og derefter hvert andet år forelægger en beretning for Europa-Parlamentet, Rådet og Det Økonomiske og Sociale Udvalg om anvendelsen af direktivet og om nødvendigt fremsætter forslag, navnlig vedrørende definitionerne i artikel 2, med henblik på at tilpasse direktivet til den tekniske og økonomiske udvikling og til resultatet af de høringer, Kommissionen foretager.

Denne rapport omhandler gennemførelsen af direktivet siden dets vedtagelse i november 1998 og frem til udgangen af 2002.

Rapporten indeholder en beskrivelse og gennemgang af de væsentligste fakta vedrørende direktivets vigtigste bestemmelser og gennemførelsen heraf i national ret. Rapporten bygger på medlemsstaternes oplysninger om gennemførelsen af bestemmelserne i national ret, de holdninger, markedets aktører har givet udtryk for, navnlig mht. udviklingen inden for piratvirksomhed og de nationale myndigheders håndhævelse af bestemmelserne, og på Kommissionens egne holdninger og analyser. Rapporten inddrager endvidere resultaterne af en uafhængig undersøgelse, der blev iværksat i 1999, om anvendelsen af adgangsstyring af andre årsager end hensynet til beskyttelse af indtjening.

Endvidere indgår rapporten i Kommissionens omfattende strategi for det indre marked, der sigter mod at fjerne hindringer for handel med tjenesteydelser.[3]

2. DIREKTIVETS BAGGRUND OG INDHOLD

2.1. Baggrund

De teknologiske fremskridt, liberaliseringen og harmoniseringen af den retlige ramme førte i de sidste ti år af det 20. århundrede til en kraftig vækst i antallet af radio- og tv-kanaler og informationssamfundets tjenester i Europa. Disse nye tjenester udbydes primært af kommercielle virksomheder og finansieres enten af

---

1 EFT L 320 af 28.11.1998, s. 54, se også http://europa.eu.int/comm/internal_market/en/media/condac/dir/index.htm.

2 28.11.1998

3 KOM(2000) 888 endelig af 29.12.2000 "En strategi for tjenester i det indre marked", se også http://europa.eu.int/comm/internal_market/en/services/services/index.htm.

reklameindtægter og sponsorering eller betaling af gebyrer og abonnement. Typiske eksempler på denne udvikling er satellitbaserede betalingstv-stationer, der tilbyder kanaler med særlig populært indhold (film) eller temakanaler om sport, livsstil eller rejser.

For at sikre betaling for de tjenester, de leverer, anvender udbyderne såkaldte adgangsstyringsteknologier, der i princippet gør det umuligt at få brugbar adgang til tjenesten uden udbyderens forudgående tilladelse. Selv om en udsendelse, som er beskyttet med adgangsstyring, måske kan modtages mange steder, kan den kun ses/høres, hvis seeren/lytteren benytter en særlig dekoder, ofte sammen med et smart card[4], som er købt hos tjenesteudbyderen. Denne metode er overordentlig effektiv til at sikre betalingen, forudsat at kun de borgere, der har betalt for tjenesten, og som udbyderen derfor søger at nå, er i stand til at dekode den pågældende tjeneste.

I dag findes der ca. 126 satellitbaserede tv-kanaler. Halvdelen af disse kanaler er krypteret med 12 forskellige adgangsstyringssystemer.

Satellit	Platform	Adgangsstyringssystem	Hovedmarked
Astra	BSkyB	Videoguard	Det Forenede Kongerige, Irland
Astra	Canal Satélite Digital	Mediaguard	Spanien
Astra	CanalSatellite	Mediaguard; Viaccess	Frankrig
Astra	CanalDigitaal	Irdeto; Mediaguard	Nederlandene
Astra	Première World	Betacrypt	Tyskland, Østrig
Astra	Wizja TV	Cryptoworks	Polen
Astra	UPC Direct	Cryptoworks	Ungarn
Astra	UPC Direct	Cryptoworks	Tjekkiet, Slovakiet
Eutelsat	Tele+ Digitale	Mediaguard; Videoguard	Italien
Eutelsat	Absat	Viaccess	Frankrig, Belgien, Luxembourg
Eutelsat	TPS	Mediaguard; Viaccess	Frankrig
Eutelsat	Stream	Mediaguard; Videoguard	Italien
Eutelsat	Alpha Digital	Nagravision	Grækenland, Cypern
Eutelsat	Nova	Irdeto	Grækenland, Cypern
Eutelsat	Cyfra+	Mediaguard	Polen
Eutelsat	Polsat	Nagravision	Polen
Hispasat	TV Cabo	Nagravision	Portugal
Hispasat	Via Digital	Nagravision	Spanien
Sirius	Viasat	Viaccess	Skandinavien
Thor	Canal Digital	Conax	Skandinavien

Tabel 1: Primære udbydere af satellitbaseret betalingstv i Europa (2002)

Adgangsstyring er et udvalg af teknologier, som kan anvendes og også i praksis bliver anvendt til flere formål. Ud over at sikre betalingen for selve tjenesten bruges adgangsstyring også ofte samtidig til at indsnævre den potentielle målgruppe til et bestemt geografisk område, f.eks. af ophavsretlige årsager, eller til en bestemt brugergruppe, f.eks. ved at forhindre adgang for mindreårige.

Fremkomsten af betalingstv har også givet grobund for en blomstrende kommerciel piratindustri. Ulovlig adgang til en tjeneste, som er beskyttet med adgangsstyring, har en række negative konsekvenser for den berørte tjenesteudbyder. Piratvirksomhed betyder, at udbyderne mister deres indtjening, og er en direkte

[4] Smart cards eller "chipkort" er plastkort på størrelse med et kreditkort med en indbygget mikroprocessor og hukommelse, som er i stand til at behandle data. Grundlæggende er smart cards små, bærbare og ofte sikrede computere.

trussel mod de berørte udbyderes økonomiske bæredygtighed, mod den indbyrdes konkurrence og dermed mod et varieret udbud af tjenester for offentligheden.

Teknologi alene kan ikke løse hele problemet med piratvirksomhed.[5] For at bekæmpe piratvirksomhed har nogle medlemsstater indført ny lovgivning parallelt med de tekniske modforanstaltninger, som tjenesteudbyderne har truffet. Andre har forsøgt at anvende de gældende bestemmelser i strafferetten, konkurrenceretten eller erstatningsretten. Nogle medlemsstater havde overhovedet ingen retlig beskyttelse på området. I 1995 påviste Kommissionen i en undersøgelse[6] en række væsentlige forskelle mellem medlemsstaternes retlige beskyttelse, for så vidt angår omfang, forbud og sanktioner. Efter en omfattende høringsproces foreslog Kommissionen at harmonisere den retlige beskyttelse af enhver elektronisk tilvejebragt tjeneste, der benyttede en form for adgangsstyring til at sikre tjenestens indtjening. I slutningen af 1998 blev direktiv 98/84/EF[7] vedtaget.

2.2. Direktivets vigtigste bestemmelser

Direktivet sigter mod at bekæmpe piratvirksomhed mod "beskyttede tjenester" ved at forbyde kommercielle aktiviteter med relation til "ulovlige anordninger". En sådan retlig beskyttelse bygger på princippet om at dæmme op for det ulovlige kommercielle marked for dekodere "tidligt i forsyningskæden", dvs. at hindre slutbrugernes adgang til ulovlige dekodere og beslægtet udstyr. Denne fremgangsmåde fungerer godt, hvis interesserede slutbrugere ikke råder over den specialiserede teknologi og viden til at fremstille ulovlige dekodere og smart cards.

Direktivet konsoliderer desuden det indre markeds funktion ved ikke at give medlemsstaterne mulighed for at indskrænke den frie bevægelighed for anordninger til adgangsstyring eller det frie udbud af betalingstjenester af årsager, som er relateret til de pirataktiviteter, som nævnes i direktivet.

2.2.1 Definitioner

Beskyttet tjeneste

Direktivet omfatter ikke kun konventionelle tv- og radiospredningstjenester, men også alle former for interaktive onlinetjenester (informationssamfundstjenester[8]). Tjenester skal forstås som defineret i traktatens artikel 50 (tidl. artikel 60)[9] som

---

5 Allerede i 1991 konkluderede Europarådet, at den tekniske beskyttelse måtte suppleres med passende retlige foranstaltninger, se Ministerudvalgets henstilling R (91) 14 om retlig beskyttelse af krypterede fjernsynsprogrammer, http://cm.coe.int/ta/rec/1991/91r14.htm.

6 KOM(96) 76 endelig udg. af 6.3.1996 – Grønbog om retlig beskyttelse af krypterede tjenester i det indre marked, se også http://europa.eu.int/comm/internal_market/en/media/condac/dir/legproc_en.htm.

7 Direktiv 98/84/EF sikrer kun retlig beskyttelse af tjenester med adgangsstyring. Selve tilvejebringelsen af disse tjenester og de tekniske krav til lovlige anordninger til adgangsstyring er omfattet af andre fællesskabsdirektiver, herunder direktiv 2002/19/EF (adgangsdirektivet) og 2002/22/EF (forsyningspligtdirektivet), EFT L 108 af 24.4.2002, http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm.

8 Informationssamfundstjenester er defineret i artikel 1, stk. 2, i Europa-Parlamentets og Rådets direktiv 98/48/EF af 20. juli 1998 om ændring af direktiv 98/34/EF om en informationsprocedure med hensyn til tekniske standarder og forskrifter, EFT L 217 af 5.8.1998, s. 18.

9 Ved "tjenesteydelser" i denne traktats forstand forstås ydelser, der normalt udføres mod betaling, i det omfang de ikke er omfattet af bestemmelserne for den frie bevægelighed for varer, kapital og personer.

fortolket af EF-Domstolen.[10] Direktivet beskytter "indholdstjenester" uanset de tekniske kendetegn ved den anvendte udsendelsesmetode. Direktivet er det første fællesskabsdirektiv, der gælder for både radio/tv-spredningstjenester og interaktive tjenester. Det kan opfattes som det første eksempel på "retlig konvergens"[11] i EU-lovgivningen.

For at kunne opnå den beskyttelse, som direktivet tilvejebringer, skal tjenesterne dog benytte en eller anden form for adgangsstyring med det formål at sikre den berørte tjenesteudbyder et vederlag. Dette kan ske ved at betale et abonnement (der f.eks. giver adgang til at se det fuldstændige programudbud på en bestemt kanal i en aftalt periode) eller ved at betale et licensgebyr (f.eks. for at se én bestemt film). Formålet med en sådan betaling direkte til tjenesteudbyderen er at sikre tjenestens[12] økonomiske bæredygtighed. Forretningsmodeller, hvorved en bestemt tjeneste udbydes mod betaling af et vederlag fra modtagerens side, men hvor også supplerende tjenester udbydes uden direkte betaling, men med adgangsstyring, er ligeledes omfattet (f.eks. "bonusnumre", som kan hentes på internet af lovlige ejere af en original musikcd). Uden denne sammenhæng mellem vederlaget og en tjeneste, som er beskyttet med adgangsstyring, kan der ikke ydes nogen retlig beskyttelse i henhold til direktivet.

Udbuddet af adgangsstyring til radio-, tv- og informationssamfundstjenester, der i direktivet benævnes en selvstændig adgangsstyrende tjeneste, er ligeledes omfattet af begrebet "beskyttet tjeneste". Selv om udbydere af sådanne tjenester ikke har nogen direkte økonomisk interesse i de "indholdstjenester", som tjenestens adgangsstyring beskytter, har udbyderen en umiddelbar økonomisk interesse i at beskytte den sikkerhed, som adgangsstyringen tilbyder. Vellykket piratvirksomhed over for en sådan beskyttelsesteknologi underminerer direkte kundernes tillid til den pågældende tjenestes beskyttelsesevne og derved også dens økonomiske bæredygtighed.

Adgangsstyring

Direktivet er udformet teknologineutralt. Ved ikke at henvise til specifikke teknologier, men derimod at anvende overordnede, funktionelle definitioner bliver direktivet mere "fremtidssikret" og mindre "vedligeholdelseskrævende", ligesom det skaber en mere stabil retlig ramme og dermed optimal retssikkerhed.

Det omfatter ikke alene typiske teknologier til adgangsstyring baseret på kryptografi som dem, der benyttes i betalingstv, men også enhver anden teknologi, der hindrer adgang til tjenesten uden tjenesteudbyderens forudgående tilladelse, f.eks. de bruger-ID/adgangskodeordninger, der ofte anvendes af betalingstjenester på internet.

---

10 I overensstemmelse med Domstolens retspraksis er der til begrebet en tjeneste, der "normalt udbydes mod vederlag", ikke knyttet nogen specifik finansieringsmåde. Artikel 60 (nu EF-traktatens artikel 50) kræver ikke, at tjenesten betales af dem, for hvem den udføres - sag C-352/85 Bond van Adverteerders Sml. 1988, s. 2085, præmis 16 – men kræver blot, at der skal ydes et vederlag for den pågældende tjeneste - sag C-109/92, Wirth, Sml. 1993-I, s. 6447, præmis 15.

11 Kommunikations- og informationsteknologier anvender i stigende grad samme, eller i det mindste tilsvarende, typer af (digital) teknologi. Denne "teknologiske konvergens" påvirker i stadigt højere grad markeder og tjenesteudbud inden for radio-/tv-spredning, interaktive tjenester og elektronisk kommunikation, og således også den beslægtede regulering. I et sådant miljø, hvor områdegrænserne er udvisket, opfattes "juridisk konvergens", hvor juridiske instrumenter lægges sammen på baggrund af en fælles teknologineutral indfaldsvinkel, ofte som den bedste reguleringsmæssige respons.

12 Se direktivets betragtning 6.

Ulovlige anordninger

Ulovlige anordninger skal være konstrueret eller tilpasset til at give adgang i forståelig form til en beskyttet tjeneste uden tjenesteudbyderens tilladelse. Typiske eksempler på ulovlige anordninger er særligt hardwareudstyr eller særlige softwareprogrammer, der er konstrueret til at omgå adgangsstyringsbeskyttelsen. På grund af udviklingen inden for smart card-relaterede teknologier er fuldt funktionsdygtige smart cards i form af modificerede originalkort eller kopier af originalkort eller specialfremstillede, helt nye piratkort i dag de hyppigst anvendte ulovlige anordninger. Tomme smart cards eller almindelige anordninger til programmering af smart cards[13] er dog ikke i sig selv ulovlige anordninger.

2.2.2 Ulovlige handlinger

Modsat andre af direktivets afsnit er bestemmelserne om ulovlige handlinger meget konkrete. Den udførlige liste over handlinger, der er forbudt, dækker hele forretningskæden af aktiviteter, lige fra den indledende fremstilling til eftersalgs-vedligeholdelse og reparation af ulovlige anordninger, herunder alle former for kommerciel kommunikation.[14]

Sanktionerne efter direktivet er kun rettet mod kommercielle handlinger, der åbner mulighed for uautoriseret modtagelse[15], og ikke mod uautoriseret modtagelse som sådan. Direktivet afspejler klart et ønske om at standse piratvirksomhed "tidligt i forretningskæden", dvs. ved de handlinger, der åbner mulighed for ulovlig adgang.

2.2.3 Sanktioner og retsmidler

Direktivet pålægger ikke medlemsstaterne at indføre specifikke sanktioner, men fastslår kun, at sanktionerne skal være effektive, afskrækkende og stå i et rimeligt forhold til den ulovlige handlings potentielle virkning[16]. Direktivet fastlægger hverken sanktionernes omfang eller type[17], ligesom det ikke på forhånd forudser anvendelse af specifikke bestemmelser i den nationale strafferet[18].

Medlemsstaterne skal stille et udvalg af passende retsmidler til rådighed for udbydere af "beskyttede tjenester", herunder som minimum muligheden for at anlægge erstatningssag, opnå nedlæggelse af påbud eller forbud eller andre præventive foranstaltninger og om nødvendigt mulighed for, at ulovlige anordninger kan tages ud af erhvervsmæssig omsætning.

---

13 En anordning til programmering af smart cards er en hardwareanordning, som er tilsluttet og styres af en pc, og som er i stand til at indlæse data i smart card'ets hukommelse.

14 Det fastlægges i betragtning 14, hvad dette begreb omfatter, et begreb, som på tidspunktet for vedtagelsen af direktivet, endnu ikke eksisterede i fællesskabsretten.

15 I direktivets betragtning 13 tydeliggøres begrebet "i kommercielt øjemed", idet der specifikt henvises til "direkte og indirekte økonomisk gevinst".

16 Denne fremgangsmåde anvendes almindeligt i lovgivning vedrørende det indre marked. Den er fastsat i Kommissionens meddelelse om betydningen af sanktioner for gennemførelsen af fællesskabslovgivningen - KOM(95) 162 - og Domstolen har for første gang tilsluttet sig den i dommen i sag 68/88, Kommissionen mod Grækenland, Sml. 1989, s. 2965.

17 Det fremgår af betragtning 23, at medlemsstaterne ikke er forpligtet til at fastsætte strafferetlige sanktioner.

18 Betragtning 22 giver eksempelvis mulighed for en "videntest" ved ulovlige aktiviteter. Betragtning 23 tillader for eksempel beslaglæggelse af ulovlige anordninger.

2.3. Spørgsmål rejst under vedtagelsen af direktivet

2.3.1 Anvendelse af adgangsstyring af andre grunde end for at sikre tjenesteudbyderens vederlag

Teknologier til adgangsstyring styrer og sikrer adgangen til elektronisk transmitterede "indholdstjenester". Disse teknologier giver brugerne mulighed for at fastslå præcist, hvilke betingelser der gives adgang på.

Direktivet beskytter udelukkende tjenesteudbydere, der anvender adgangsstyring til at sikre, at de får betaling. Adgangsstyring kan dog tjene og tjener da også i praksis mange andre formål. De fleste systemer til adgangsstyring, som anvendes af udbydere af satellitbaseret betalingstv, sikrer ikke alene betalingen, men tjener også til at indsnævre den potentielle målgruppe for en udsendelse til et bestemt geografisk område (ofte en medlemsstat), typisk af ophavsretlige årsager. Adgangsstyring anvendes desuden til at beskytte mindreårige mod anstødeligt indhold.

I forbindelse med direktivets vedtagelse var der en bred debat om, hvorvidt der var behov for og hvor klogt det var at udvide omfanget af den retlige beskyttelse, som direktivet sikrer, til også at omfatte anvendelsen af adgangsstyring af ophavsretlige årsager. En sådan udvidelse ville give ophavsrethaverne ret til - parallelt med og uafhængigt af udbyderne af de beskyttede tjenester - at rejse sager mod og kræve erstatning fra fabrikanter og forhandlere af ulovlige anordninger.

I sidste ende blev det besluttet ikke at lade direktivet omfatte ophavsretsbeskyttelse. En af hovedårsagerne var, at efter den dagældende fællesskabsret kunne fremstilling og salg af ulovlige anordninger ikke betragtes som en overtrædelse af ophavsretten[19]. En anden grund var de igangværende forhandlinger om et udkast til direktiv om ophavsret i informationssamfundet, der indeholdt bestemmelser om tekniske beskyttelsesforanstaltninger og hindring af omgåelse, og som blev betragtet som et supplement til direktivet om adgangsstyring.[20]

Kommissionen indvilligede i at udføre en undersøgelse af de retlige og økonomiske konsekvenser af anvendelsen af adgangsstyring af andre årsager end beskyttelse af vederlag.[21] Undersøgelsen, som blev afsluttet i april 2000, satte fokus på "interesser, som ikke er rettet mod ydelsen af nogen form for direkte økonomisk vederlag fra modtagerens side til gengæld for tjeneste-/indholdsudbyderens levering af en tjeneste".

Undersøgelsen kortlagde en række sådanne interesser, spændende fra overholdelse af kontraktlige og lovbestemte forpligtelser og til markedsførings- og reklamestrategier, sikkerhedsaspekter og indirekte vederlag. I alle tilfælde blev det konkluderet i undersøgelsen, at beslutningen om at anvende adgangsstyring byggede på gyldige økonomiske og retlige overvejelser. Nogle af disse interesser fandtes oftest hos radio-/tv-stationer, andre hos udbydere af informationssamfundets tjenester. Dette

---

19 Det anføres i direktivets betragtning 21, at anvendelsen af Fællesskabets regler for intellektuel ejendomsret ikke berøres af direktivet.

20 Se KOM(97) 628 endelig udg. af 10.12.1997, s. 33.

21 Institut for Informationsret (IVIR) på Amsterdams Universitet fik i opdrag at udføre undersøgelsen. Den endelige rapport fra april 2000 findes på: http://www.ivir.nl/publications/other/ca-report.htm eller på: http://europa.eu.int/comm/internal_market/en/media/condac/backgrnd/index.htm.

viser, at der ofte er flere grunde på én gang til at anvende adgangsstyring. Det lader til, at kravene fra indholdsindustrien (ophavsret) og anvendelsen af geografisk bredt dækkende spredningsteknikker (satellit) er de primære drivkræfter bag anvendelsen af adgangsstyring til andre formål end sikring af vederlag.

I undersøgelsen forudses det, at anvendelsen af adgangsstyring af andre årsager end sikring af vederlag vil tiltage, men at det stadig er for tidligt at give et seriøst og pålideligt bud på, hvordan markedet vil udvikle sig, og hvilken indvirkning øget anvendelse af adgangsstyring vil få. Undersøgelsen viser, at risikoen for at blive udsat for piratvirksomhed vil være den samme, både hvor adgangsstyringen anvendes til at sikre vederlag, og hvor den anvendes til andre formål.

2.3.2 Kommercielt øjemed over for privat

Listen over ulovlige handlinger, som findes i direktivet, bygger primært på listen over ulovlige handlinger i Europarådets henstilling R (91) 14. [22] Det er opfattelsen i dette direktiv og i henstillingen, som er direktivets begrebsmæssige forgænger, at den mest effektive måde at hindre piratvirksomhed på er ved at koncentrere sig om de kommercielle handlinger, der åbner mulighed for ulovlig adgang.

Da direktivet blev forhandlet på plads, havde nogle få medlemsstater dog indført forbud mod visse private handlinger som f.eks. privat besiddelse af ulovlige anordninger og/eller selve den uautoriserede private modtagelse. Under forhandlingerne om direktivet var der forskellige opfattelser blandt medlemsstaterne og Fællesskabets institutioner, for så vidt angår behovet for og det hensigtsmæssige i at udvide harmoniseringen af definitionen af ulovlige handlinger til at omfatte andet end kommercielle handlinger. I sidste ende blev det besluttet, at direktivet kun skulle omfatte kommercielle handlinger, men at det i henhold til national ret skulle være muligt for medlemsstaterne at forbyde privat besiddelse af ulovlige anordninger.[23]

Der blev ført lignende drøftelser i forbindelse med vedtagelsen af direktivet om ophavsret i informationssamfundet, som endte med en mere eller mindre lignende løsning.[24]

3. DIREKTIVETS GENNEMFØRELSE

3.1. Meddelelse om gennemførelsesforanstaltninger

Direktivet gav medlemsstaterne en periode på halvandet år til at gennemføre direktivets bestemmelser i national ret. Da gennemførelsesfristen udløb, dvs. den 28. maj 2000, havde kun meget få medlemsstater givet Kommissionen meddelelse om de gennemførelsesbestemmelser, de havde vedtaget.

I overensstemmelse med proceduren i traktatens artikel 226 (tidligere artikel 169) for manglende meddelelse om nationale gennemførelsesforanstaltninger blev der sendt åbningsskrivelser til de medlemsstater, der ikke havde meddelt Kommissionen deres

---

22 Nærmere oplysninger findes i kapitel 6 i denne rapport.

23 Se direktivets betragtning 21.

24 Nærmere oplysninger fås i artikel 6, stk.1, 2 og 3, og betragtning 49 i direktiv 2001/29/EF, EFT L 167 af 22.6.2001, s. 10.

gennemførelsesbestemmelser. Herefter gav et stort flertal af medlemsstaterne meddelelse om deres gennemførelsesforanstaltninger.

På datoen for denne meddelelse er Kommissionen blevet pålagt at indbringe flere medlemsstater (Grækenland og Spanien) for EF-Domstolen, fordi de ikke har meddelt gennemførelsesbestemmelser.[25]

Flere af gennemførelsesmeddelelserne indeholder ikke alle de oplysninger, Kommissionen behøver for at kunne vurdere, om den nationale gennemførelse er fuldstændig og i overensstemmelse med fællesskabsretten. For at afklare denne situation bliver der i øjeblikket ført bilaterale drøftelser mellem Kommissionen og de berørte medlemsstater. Kommissionen indleder efter behov traktatbrudsprocedurer efter artikel 226 mod de medlemsstater, som efter Kommissionens opfattelse ikke gennemfører direktivet med den påkrævede nøjagtighed, præcision og klarhed.[26]

3.2. Gennemførelsen i medlemsstaterne

Der er gået ganske lang tid mellem direktivets ikrafttræden og udstedelsen af den nationale lovgivning, der gennemfører det. Størstedelen af lovgivningen trådte i kraft fra andet halvår af 2000 og derefter.

År	**Medlemsstat**
<1998	Frankrig - Nederlandene
1999	
2000	Østrig - Irland - Italien - Sverige - Det Forenede Kongerige
2001	Danmark - Finland - Portugal
2002	Tyskland - Luxembourg - Grækenland
Senere	Belgien - Spanien

Tabel 2: Ikrafttrædelsesår

En løbende ajourført oversigt over gennemførelsen af direktivet i EU-medlemsstaterne, EØS-landene og kandidatlandene, herunder omfattende referencer til national ret, samt uformelle oversættelser til engelsk, findes på EUROPA-webstedet.[27]

Som det kunne forventes, har medlemsstaterne gennemført direktivet på mange forskellige måder i national ret. Nogle har valgt at lade traditionelle radio- og tv-tjenester omfatte af medielovgivningen, mens informationssamfundets tjenester og adgangsstyrende tjenester er selvstændigt omfattet af lovgivning om cyberkriminalitet eller beslægtet lovgivning. Andre medlemsstater har foretrukket at have et enkelt (sæt) bestemmelser, der omfatter alle tjenester, under enten straffelovgivningen eller en særlovgivning.

---

25 Spanien: sag C-58/02, Grækenland: sag C-219/02, Kommissionens pressemeddelelse IP/02/455 af 22.3.2002, http://europa.eu.int/comm/internal_market/en/media/infr/02-455.htm.

26 Sag C-197/96, præmis 14 og 15.

27 http://europa.eu.int/comm/internal_market/en/media/condac/natimp/index.htmhttp://europa.eu.int/comm/internal_market/en/media/condac/natimp/index.htm.

I det store og hele stemmer de nationale gennemførelsesforanstaltninger, der er meddelt Kommissionen, overens med direktivets krav. I de fleste medlemsstater er alle beskyttede tjenester tilstrækkeligt dækkede, selv om det i nogle få medlemsstater er uklart, om adgangsstyrende tjenester i sig selv rent faktisk nyder beskyttelse. Nogle mindre uklarheder drøftes fortsat mellem Kommissionen og de berørte medlemsstater.

En lignende situation gør sig gældende, hvad angår de ulovlige handlinger, som skal forbydes i henhold til direktivets artikel 4. I nogle få tilfælde er en specifik ulovlig handling ikke udtrykkeligt forbudt, fordi den anses for at falde ind under et mere generisk begreb eller en gældende generalklausul i den nationale strafferet. For at sikre retssikkerheden for borgere og erhvervsliv drøfter Kommissionen disse sager med den berørte medlemsstat.

Selv om medlemsstaterne ikke ved direktivet bliver pålagt at indføre strafferetlige sanktioner[28], har alle medlemsstater på nær to (Italien og Portugal) indført sanktioner i form af fængsels- og/eller bødestraf for, hvad de betragter som de primære ulovlige handlinger (fremstilling og salg). Det er klart, at der på flere punkter er forskelle i, hvordan de enkelte medlemsstater fortolker de ulovlige handlingers krænkende art, og hvilken form for præventiv sanktion der kræves.

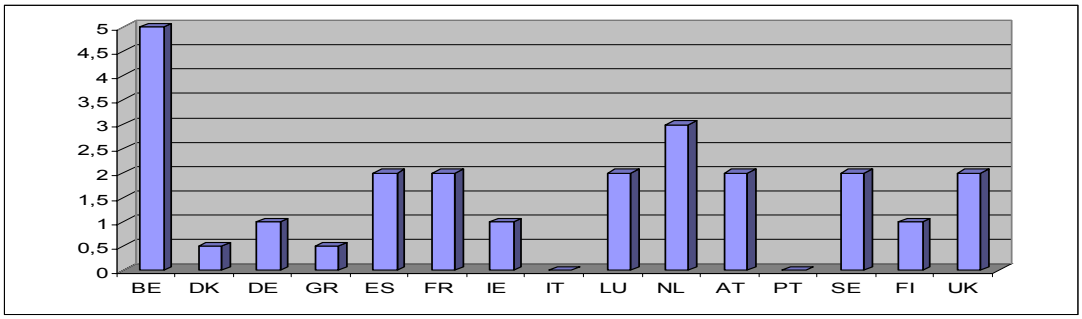


Diagram 1: Maksimal straframme i år for de primære ulovlige handlinger

Nogle få medlemsstater har indført et system af nærmere afpassede sanktioner. Ved at integrere forbud og sanktioner i strafferetten tages der også hensyn til de klassiske sekundære strafbare handlinger (medvirken, anstiftelse og meddelagtighed), ligesom der er adgang til de dertil hørende strafferetlige procedurer (ransagning og beslaglæggelse samt konfiskation).

I nogle få medlemsstater (Østrig, Tyskland og Italien), hvor de gældende retsforskrifter allerede kunne anvendes som hjemmel til at retsforfølge visse former for piratvirksomhed, har de specifikke, men mindre alvorlige sanktioner, der er indført for de i direktivet definerede ulovlige handlinger, resulteret i en faktisk begrænsning af den retlige beskyttelse i disse medlemsstater.[29]

I de fleste medlemsstater er der adgang til passende retsmidler for krænkede tjenesteudbydere. I de få tilfælde, hvor det ikke er helt klart, om der findes alle de retsmidler, der kræves ved direktivet, har Kommissionen anmodet den berørte medlemsstat om en præcisering.

---

[28] Direktivets betragtning 23, anden sætning.

[29] Lex specialis derogat generali.

Kommissionen konkluderer, at direktivet efter alt at dømme endnu ikke er fuldt gennemført i national ret i alle medlemsstater. To medlemsstater mangler stadig at afslutte den nationale gennemførelse, mens der er en vis usikkerhed med hensyn til flere andre nationale gennemførelser, for så vidt angår deres fuldstændighed og forenelighed. Kommissionen vil også fremover gennemgå de relevante nationale foranstaltninger og arbejde ihærdigt på at sikre fuld gennemførelse af direktivet.

3.3. Nationale bestemmelser, der rækker ud over direktivets krav

Direktivet indfører kun et minimumsniveau for den retlige beskyttelse mod piratvirksomhed og giver medlemsstaterne stor fleksibilitet og selvbestemmelse, når det gælder om at tilpasse deres nationale regler for bekæmpelse af piratvirksomhed til deres egne behov og politikker. Flere medlemsstater har udnyttet denne særlige ret og udvidet definitionen af beskyttede tjenester samt af ulovlige handlinger, sanktioner og retsmidler.

Ganske mange medlemsstater stiller hverken udtrykkelige krav om anvendelse af adgangsstyring eller fokuserer alene på, at tjenesteudbyderen får betaling, men beskytter alle tjenester mod uautoriseret adgang eller adgang uden tilladelse.

Tilsvarende forbyder et mindretal af medlemsstaterne personlig anvendelse og/eller privat besiddelse af ulovlige anordninger.

Nogle medlemsstater har udtrykkeligt indført specifikke sanktioner (bl.a. offentliggørelse af domme og beslaglæggelse af fortjeneste) og retsmidler (erstatning for tabt fortjeneste og overdragelse af opnået fortjeneste).

I nogle få medlemsstater har en national tilsynsførende myndighed (i visse tilfælde telemyndigheden og i andre tilfælde en særlig tjeneste) fået til opgave at overvåge og føre tilsyn med markedet og med (den delvise) håndhævelse af lovgivningen.

3.4. Udvidelsen

Kandidatlandene skal gennemføre direktivet som led i den gældende fællesskabsret. En rettidig gennemførelse og en effektiv håndhævelse er af afgørende betydning i kampen mod piratvirksomhed i EU og i fremtidige medlemsstater. Sideløbende med udbygningen af beskyttelsen i EU er der en stigende tendens til, at piratvirksomhed inden for betalingstv og internettjenester bliver forrykket mod Centraleuropa.

Udvidelsen er én af Kommissionens topprioriteter i 2002[30] og 2003[31]. Kommissionen følger aktivt gennemførelsen og bistår i videst muligt omfang kandidatlandene med udformningen og den efterfølgende praktiske indførelse af den relevante nationale lovgivning til gennemførelse af direktivet.

Selv om der stadig er behov for en stor indsats, har fremskridtene hidtil været opmuntrende. Fire lande har allerede fået det meste af den nødvendige lovgivning på plads. Flere andre kandidatlande er i færd med at udarbejde deres udkast til gennemførelsesbestemmelser og forventer at vedtage dem endelig inden udgangen af

---

30 KOM(2001) 620 endelig af 5.12.2001, s. 14.

31 Se pressemeddelelse IP/02/338 (politisk strategi for 2003).

2003. De øvrige lande har bekræftet, at de agter at vedtage de nødvendige foranstaltninger senest ved tiltrædelsen i 2004.

Som påpeget i foregående kapitel i denne rapport er det primært de nationale myndigheders opgave at sikre, at den gældende lovgivning også bliver anvendt. For at være klar til at anvende lovgivningen, når den er trådt i kraft, må de håndhævende myndigheder i kandidatlandene have undervisning.

Kandidatlandene gør opmuntrende fremskridt med gennemførelsen af direktivet, selv om der fortsat er behov for en betydelig indsats.

Kommissionen vil fortsætte samarbejdet med alle kandidatlande om at opnå et tilstrækkeligt niveau af administrativ og retslig kapacitet på tiltrædelsestidspunktet.[32] Med hjælp fra specialiserede aktører i branchen kan der afholdes specialiserede undervisningsseminarer for politi og retsvæsen.[33]

4. MARKEDSUDVIKLINGEN OG ANVENDELSEN AF DIREKTIVET

4.1. Høring af markedets parter

Som forberedelse til denne rapport gennemførte Kommissionen en høring blandt de vigtigste brancheinteressenter, som er berørt af piratvirksomhed, om tjenester, der beskyttes af adgangsstyring, og de relaterede retlige modforanstaltninger. I overensstemmelse med Kommissionens tilsagn i hvidbogen om styreformer i Europa[34] og dens nylige forslag om bedre lovgivning[35] blev denne høring gennemført for at fremme en åben dialog om de problemer med piratvirksomhed, der viser sig på markedet, og for at hjælpe med at indsamle og analysere ny og eksisterende information på det teknisk og juridisk avancerede område, som direktivet dækker. Kommissionen gennemførte ikke nogen fuldstændig konsekvensanalyse[36], eftersom der stadig blev arbejdet på at gennemføre direktivet i national ret i rapportperioden.

Høringssvarene har givet vigtig information til forberedelsen af denne rapport og den mulige opfølgning.[37] Markedsaktørerne er naturligvis ikke videre opsatte på at drøfte piratvirksomhed og dens effekt på deres aktiviteter i detaljer. Alt for stor åbenhed kan give bagslag på grund af den potentielle effekt på kundernes tillid til kvaliteten af beskyttelsen, på konkurrencesituationen på markedet og på aktionærværdien. Brancheorganisationer som AEPOC[38], STOP[39] eller ICRT[40] har vist sig at have stor

---

32 KOM(2002) 256 endelig af 5.6.2002.

33 Se også kapitel 4.3 om håndhævelse.

34 KOM(2001) 428 endelig af 25.7.2001, http://europa.eu.int/comm/governance/index_en.htm.

35 KOM(2002) 275 endelig og KOM(2002) 277 endelig udg. af 5.6.2002.

36 KOM(2002) 276 endelig af 5.6.2002.

37 Kommissionen har modtaget skriftlige bidrag fra AEPOC, EBU, AER, ACT, MPA, ACTI, ACCeS, DVD, STOP Sverige, STOP Danmark, STOP Norge, ICRT og KirchGruppe. Desuden blev der afholdt en række mere uformelle bilaterale møder med flere markedsaktører.

38 AEPOC, European Association for the Protection of Encrypted Works and Services, repræsenterer Betaresearch, BskyB, Canal+, Canal+Polska, Canal+ technologies, Conax, Eutelsat, IrdetoAccess, Motorola, NDS, NTV-Plus, Pace, Philips Digital Networks, Première, Rai, SCM Microsystems, Société Européenne des Satellites, Sogecable, Stream, Tele+, Thompson, TPS, UPC and Viaccess-France Telecom, se endvidere http://www.aepoc.org/.

39 STOP, the Scandinavian TV Organisations against Piracy, findes i Finland, Sverige, Norge og Danmark (http://www.stop.dk).

betydning for formidling af problemstillingerne og illustration af de problemer, som de medlemmer, de repræsenterer, møder. Selv om det er forståeligt, vanskeliggør en sådan protektionistisk holdning indsatsen for at få et klart overblik over omfanget og følgerne af problemet og for at finde egnede og effektive løsninger.

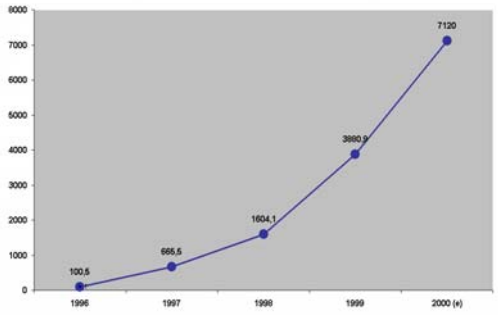
I tråd med indsatsen for at kommunikere mere aktivt med offentligheden om europæiske problemstillinger har Kommissionen fuldstændig omlagt sine websteder på EUROPA med relation til direktivet og dets gennemførelse.[41]

4.2. Bekæmpelse af pir@tvirksomhed - et mål i bevægelse

Audiovisuel piratvirksomhed, især piratvirksomhed relateret til betalingstjenester, udvikler sig i tråd med de tjenester, den søger at udnytte. I starten var det muligt at hacke sig ind på krypterede analoge betalingstv-kanaler ved hjælp af modificerede dekodere. Denne form for piratvirksomhed krævede specialviden om analog tv-teknologi og elektronik samt særlige fabrikationsfærdigheder.

Tjenester, der udgør mål for pirater

Digitaliseringen gav en enorm vækst i distributionskanaler og forsyningen af indhold, hvilket bl.a. har skabt et marked for digitalt betalingstv, der er i hastig udvikling. Indtjeningen fra abonnementer er vokset eksponentielt siden 1996. Ifølge Kommissionens seneste undersøgelser tegnes der stadig flere abonnementer. Indtjeningen fra digitale tv-abonnementer er steget fra under 25 % af brancheindtjeningen i 1995 til ca. 35 % i 2000.



Kilde: IDATE og den syvende gennemførelsesrapport vedrørende telekommunikationssektoren

Diagram 2: indtjeningen fra digitale tv-abonnementer siden 1996 (mio. EUR)

Med analoge kabelnet og landbaserede fjernsynsstationers overgang til digital teknologi udbydes digitale betalingstv-tjenester i stigende grad via disse nye distributionskanaler (se tabel 3 for yderligere oplysninger). De seneste statistikker bekræfter mere eller mindre denne tendens og viser, at i 2008 vil 73 % af de europæiske hjem (122 mio. husstande) have digitalt tv[42].

Udbredelsen af digitalt tv vil føre til bred anvendelse af digitale dekodere, enten i hardwarebaseret form (dekoderbokse og intelligente tv-apparater) eller i softwarebaseret form (specialiseret software på en pc med et DVB-kort[43]).

---

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

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

42 Strategy Analytics, 28. maj 2002, http://www.strategyanalytics.com/press/prsk012.htm.

43 Et DVB-kort er computerhardware, som er konstrueret til at modtage, dekode og vise digitalt fjernsyn i overensstemmelse med de europæiske DVB-standarder på en almindelig personlig computer.

Den negative side ved denne tekniske konvergens er, at den aktuelle digitale satellittv-piratvirksomhed vil sprede sig til de nye områder som digitalt, landbaseret tv og digitalt kabeltv og blive stadig mere udbredt.

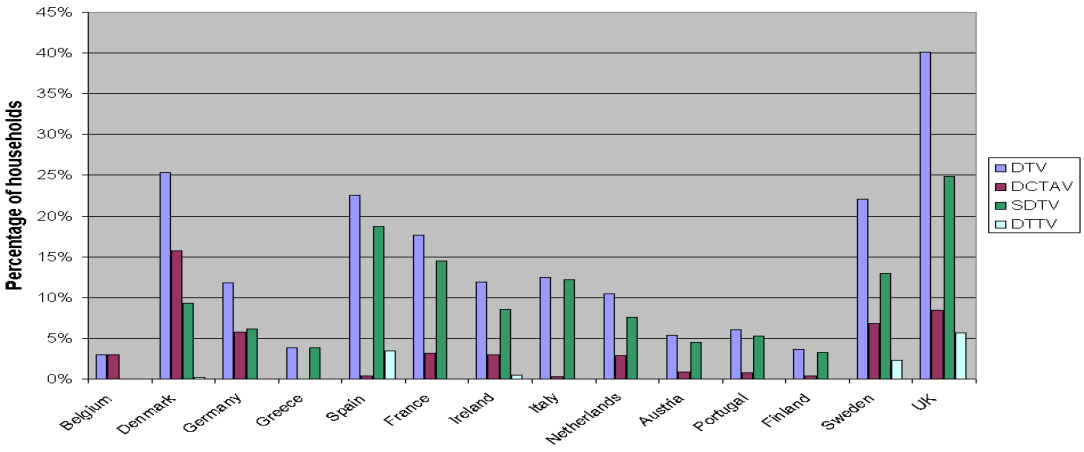
Husstande med digitalt tv	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Satellit											
Husstande med digitalt satellittv (mio.)	0,0	0,4	1,9	4,1	8,3	14,3	19,2	24,0	28,2	32,3	35,9
Kabel											
Husstande med digitalt kabeltv (mio.)	0,0	0,0	0,1	0,8	1,7	3,2	6,1	10,7	16,3	22,5	28,8
Landbaseret											
Husstande med digitalt landbaseret tv (mio.)	0,0	0,0	0,0	0,0	0,5	1,3	2,1	3,5	5,1	7,1	8,8
HUSSTANDE MED DIGITALT TV I ALT (mio.)	0,0	0,4	2,0	5,0	10,5	18,7	27,4	37,8	48,7	60,1	70,8

Kilde: Strategy Analytics, februar 2001 og den syvende gennemførelsesrapport vedrørende telekommunikationssektoren

Tabel 3: Husstande i EU med digitalt tv (plus Norge og Schweiz), tendenser og prognose

De nationale markeder for digitalt tv befinder sig på vidt forskellige udviklingstrin i medlemsstaterne. Forskellene mellem, hvor udbredte de enkelte mekanismer til levering af digitalt tv er, vil have indvirkning på omfanget af piratvirksomhed i de enkelte medlemsstater (se diagram 3 for yderligere oplysninger).

Modsat betalingstv er betalingsradiotjenester endnu ikke så udbredte i Europa. I Europa er radiospredningen primært baseret på frit-i-luften-forretningsmodeller.[44] I USA drives der nogle få betalingsradiostationer, men det sker kun på basis af særlige modtager- og adgangsstyringsteknologier. Disse stationer promoverer deres betalingstjenester ved at fremhæve den høje lydkvalitet, kyst-til-kyst-dækningen og det store udvalg af reklamefri musik-, sports- og nyhedsprogrammer. I Europa har man endnu ikke gjort tilsvarende erfaringer, selv om der i fremtiden ventes digitale betalingsradiostationer, f.eks. kombineret med anden teknologi såsom mobiltelefoni.



Kilde: Udarbejdet af Europa-Kommissionen på baggrund af data fra Strategy Analytics

DTV: Digitalt TV
DCATV: DTV via kabel
SDTV: DTV via satellit
DTTV: Digitalt landbaseret tv

Diagram 3: Udbredelsesgraden for digitalt tv blandt europæiske husstande i 2001, pr. medlemsstat og leveringsmekanisme (i % af husstande)

44 Fra tid til anden er tematiske radiokanaler kun tilgængelige for brugere, der abonnerer på de dyreste programpakker. Et eksempel findes på: http://www4.telepiu.it/v4_intrattenimento/multimusica/multimusica.asp.

Med den negative udvikling i internetøkonomien og det svage reklamemarked lancerer udbydere af informationssamfundets tjenester topkvalitetstjenester mod gebyr for at generere alternative indtægtskilder og opbygge langvarige kundeforhold gennem understøtning af kundernes digitale livsstil. Sådanne abonnementbaserede internettjenester beskyttes primært af brugernavn/adgangskode-mekanismer og spænder fra onlinespil, avancerede dokumentsøgninger, onlineudbud af hele aviser og specialiserede fagtidsskrifter og til on-demand download af musik og film. Et eksempel på en sådan blomstrende kategori af betalingstjenester er de onlineopdateringstjenester, som er til rådighed for ejere af originale softwareprogrammer, hvor den originale cd's serienummer fungerer som adgangstilladelse. Markedsaktører og lovgivere følger i øjeblikket med stor interesse disse første og formentlig endnu umodne forsøg på at generere indtægter fra onlineindholdsudbud.

Metoder og redskaber til piratvirksomhed

Det meste af den moderne piratvirksomhed mod digitalt tv er rettet mod smart cards eller dekodersoftware. Et omfattende udvalg af websteder og elektroniske opslagstavler giver detaljeret baggrundsinformation om de forskellige systemer til adgangsstyring, vejledning i (om)programmering af smart cards og henvisninger til steder, hvor man "finder" vigtigt nøglemateriale. Smart card-teknologien hører i dag til blandt de almindelige erhvervsapplikationer. Hardware- og softwareredskaberne til programmering af disse kort er lettilgængelige, fordi smart cards og deres programmeringsredskaber også bruges til lovlige formål. Det er klart, at de nødvendige redskabers brugervenlighed og adgangen til viden og information via internet har gjort det meget lettere at udøve piratvirksomhed mod digitale systemer.

Piratudgaver af smart cards er ofte baseret på de originale smart cards, udstedt af udbyderne af betalingstv. Deaktiverede kort eller kort, der kun giver adgang til det grundlæggende tjenesteudbud, ændres (såkaldte MOSC'er[45]) til kort, der giver fuld adgang til hele tjenesteudbuddet. Digitale piratudgaver af smart cards, der ofte betegnes DPSC'er, er enten funktionelt identiske "kloner" af originale kort eller nyprogrammerede smart cards.

Professionelle pirater er veludstyrede og fremstiller MOSC'er og DPSC'er i stort tal. En sådan halvindustriel produktion og distribution af piratkort kræver meget "professionelle", erhvervsmæssige arbejdsmetoder, som ofte involverer organiseret kriminalitet.

Mindre erhvervsmæssig, men ikke desto mindre lige så skadelig er den "lokale" fremstilling i langt mindre omfang af piratudgaver af smart cards på basis af offentligt tilgængelige tomme smart cards. Denne form for piratvirksomhed bruger "gør-det-selv-hardware" og information, som hovedsagelig skaffes via internet. De opnår fortjeneste ved at sælge tomme kort og programudstyr eller fuldstændige satellitmodtagelsesinstallationer, inklusive et forfalsket adgangskort[46] til fordelagtige priser. Disse pirater anvendes ligeledes af den organiserede kriminalitet som distributionskanal for piratkort fremstillet af professionelle pirater. Ofte er det

---

45 Modified Original Smart Card.

46 De marginale omkostninger ved produktion af et sådant kort er ubetydelige (mindre end 1 %) i forhold til abonnementets reelle pris.

vanskeligt at fastslå, at denne form for piratvirksomhed er kommerciel, fordi beregnende lovbrydere reducerer deres "strafeksponering" til et minimum.

Privatpersoner deltager også i denne "køkkenbords-piratvirksomhed". Som "lejlighedspirater" bruger de den samme hardware og information og tilbyder "hjemmelavede" kort som en tjeneste til venner, naboer eller kolleger, ofte mod penge eller andre værdigenstande som f.eks. piratkopier af software, musikcd'er eller dvd'er.

I stigende omfang fremstiller teknisk krævende seere selv piratkort til eget brug. Alt, hvad de behøver gøre, er at erhverve den nødvendige knowhow fra hackerwebsteder og foretage en beskeden engangsinvestering i den basale hardware.

To relativt nye og meget farlige former for piratvirksomhed er under hastig udvikling. Den første er baseret på almindelige pc'er udstyret med DVB-tv-kort og softwaredekodere. Disse kraftige softwaredekodere, som emulerer hardwaremoduler og smart cards til adgangsstyring, distribueres via internet. Den anden form består i at ændre kommercielt tilgængelige, almindelige grænsefladebaserede moduler til adgangsstyring (CAM'er) v.hj.a. specialiserede software-"lapper", der gør, at der ikke længere kræves et gyldigt smart card (såkaldte FreeCams). Begge former bygger på den meget brugervenlige distribution via internet, hvilket gør dem til potentielle piratvåben.

Alle pirater, måske bortset fra de mest professionelle, er afhængige af adgangen til nøgler, omgåelsesredskaber og anvisninger osv. på private hackerwebsteder. Disse websteder er det afgørende led i piratvirksomhedens forretningskæde, fordi de er kilden til det nødvendige materiale. Derfor er de også akilleshælen for en stor del af piratvirksomheden. Mange af disse hackerwebsteder præsenterer sig selv som private initiativer uden økonomisk støtte fra kommercielle partnere. Selv om dette muligvis er sandt for nogles vedkommende, benytter andre bannerreklamer eller anbefaler bestemte varemærker, hvilket tyder på en eller anden form for kommerciel forbindelse. Websteder kræver værtscomputere og internetforbindelser, og de er ikke gratis.

Skader forårsaget af piratvirksomhed

Audiovisuel piratvirksomhed er ikke "offerløs" kriminalitet. De fleste udbydere af betalingstv drives inden for snævre økonomiske rammer. Forskellen mellem kommerciel succes og konkurs er normalt meget lille i denne nye branche og afhænger ofte af en stadigt voksende abonnentkreds og ARPU.[47] Antallet af piratseere, der benytter tjenesterne uden at betale for det, kan udgøre hele forskellen.

Ikke alene betyder piratvirksomhed, at udbyderne mister indtægter, den øger også driftsomkostningerne og behovet for yderligere investeringer. Kilder i branchen hævder, at udskiftning af et enkelt smart card som led i en storstilet kortombytning koster ca. 11 EUR.[48] En førende betalingstv-udbyder hævdede at have brugt over 35

---

47 Average Revenue Per User (gennemsnitlig indtjening pr. bruger).

48 New Media Markets - 31.5.2002, s. 6.

mio. EUR til at udvikle sit udbredte dekoder-"middleware" og adgangsstyrings-system.[49]

Piratvirksomhed har desuden en negativ effekt på statens indtægter. Pirater betaler ikke skat af deres tjenester, og lovlydige udbydere betaler mindre moms og lavere selskabsskatter på grund af lavere omsætning og lavere fortjeneste.

Lovlydige forbrugere kan let blive vildledt om dekoderes og smart cards' oprindelse. De er de første, der mærker konsekvenserne af piraternes ulovlige adfærd, når udbyderen deaktiverer sit pirat-smart card eller træffer andre modforanstaltninger.

Endvidere forvrider piratvirksomheden også andre audiovisuelle markeder. Den påvirker ikke alene detailmarkedet for dekoderbokse og abonnementer, men har også en potentielt skadelig effekt på biografsektoren og udlejningen af videokassetter eller dvd'er på grund af adgangen til nyt kvalitetsmateriale via ulovlig adgang til elektroniske betalingstjenester.

Ifølge oplysninger fra AEPOC[50], European Association for the Protection of Encrypted Works and Services, blev der i 1996 tabt over 200 mio. EUR i fortjeneste i Europa på grund af piratvirksomhed. AEPOC anslår, at på grund af den øgede årlige lovlige omsætning hos udbydere af betalingstv er den årlige ulovlige omsætning i forbindelse med piratvirksomhed i størrelsesordenen 1 mia. EUR. For nylig anslog ITV Digital, at selskabet mistede over 100 mio. GBP i indtægter på grund af piratvirksomhed over for smart cards.[51]

Ud over den økonomiske skade, piratvirksomhed påfører, er det også forbundet med "samfundsmæssige" skader. Forbrydelser som indbrud og tyveri er pr. definition uacceptabelt i et civiliseret samfund, fordi de angriber selve kernen i vort værdisystem. Cybermodstykkerne til disse kriminelle handlinger og den skade, de forvolder på offentlighedens interesser, bør opfattes på samme vis.

Modforanstaltninger

Udbydere af betalingstv har længe arbejdet på at bekæmpe piratvirksomhed. I de første år med betalingstv afholdt udbyderne sig fra at indbringe sagerne for retten, så offentligheden ikke blev opmærksom på, hvor sårbare tjenesterne er. Det første svar på piratvirksomhed er derfor traditionelt tekniske modforanstaltninger. I dag udnytter udbyderne alle de muligheder, der ligger i deres driftssystemer, for at tilbyde modforanstaltninger, herunder opdatering af nøgler og blokering af kendte piratudgaver af smart cards.

Udbyderne overvåger desuden løbende og rutinemæssigt piratmarkedet, ligesom de analyserer nye anordninger og metoder til piratvirksomhed for at holde sig på forkant med piratvirksomheden og gå til modangreb på den. De gør systemerne mindre sårbare ved at forbedre krypteringen og udbygge de nøgleordninger, de anvender til at identificere (individuelle) brugere. Senest er flere større udbydere begyndt at udskifte alle lovlige smart cards med sikrere udgaver. En sådan ombytning af

---

49 New Media Markets - 15.3.2002, s. 5.

50 http://www.aepoc.org/

51 New Media Markets - 15.3.2002, s. 5.

millioner af kort er en stor logistisk udfordring for udbyderne, og de omkostninger, det er forbundet med, vidner om udbydernes vilje til at bekæmpe piratvirksomhed.

Der er dog praktiske grænser for denne indsats på grund af de omkostninger, det er forbundet med, generne for lovlige brugere og de tekniske muligheder ved det berørte system. På dette stadium kommer en effektiv håndhævelse af den retlige beskyttelse til at danne den næste forsvarslinje.

4.3. Håndhævelse

De fleste medlemsstater har først for nylig afstemt deres nationale lovgivning efter direktivet. Det er derfor fortsat lidt for tidligt at søge at få komplet overblik over de praktiske konsekvenser af denne nye lovgivning om piratvirksomhed og bekæmpelse heraf. De nationale retshåndhævende myndigheder og de berørte aktører i branchen skal vænne sig til den nye retlige ramme og finde ud af, hvordan de bedst kan udnytte mulighederne.

Flere af de markedsaktører, der deltog i Kommissionens høringer, udtrykte bekymring over de mange lappeløsninger i forbindelse med gennemførelsen af direktivet og de nationale retshåndhævende myndigheders modvilje mod at undersøge og retsforfølge mistænkte overtrædere. De peger på, at audiovisuel piratvirksomhed er en teknisk og juridisk kompliceret lovovertrædelse og fremhæver behovet for og deres vilje til at samarbejde, bistå og om nødvendigt undervise de nationale myndigheder i en fælles indsats. Flere eksempler på vellykket samarbejde mod pirater har vist, at en sådan strategi kan fungere og bør tilskynde myndigheder og tjenesteudbydere, der endnu ikke deltager i samarbejdet, til at involvere sig i denne gensidigt nyttige strategi. Det praktiske samarbejde bør opnås ved at afholde kursusseminarer, etablere dynamiske net af personer og myndigheder, som er involveret i kampen mod denne form for piratvirksomhed, og udveksle viden om bedste praksis og information i hele det udvidede EU[52].

De fleste bidragydere understreger de radikale forandringer af piratvirksomheden på grund af internet samt bekymringen over, at den nuværende retlige ramme ikke er udarbejdet med tanke for denne form for trussel. Det er ofte vanskeligt at påvise det kommercielle aspekt ved de forskellige hackersites. Det nødvendige nøglemateriale er umiddelbart tilgængeligt på internet, hvilket gør det muligt for enkeltpersoner at yde piratvirksomhedstjenester for venner, som oftest uden kommercielt øjemed. De klager over, at tomme kort og programmeringsredskaber kun under meget specifikke omstændigheder kan betragtes som ulovlige anordninger. Beregnende pirater er bevidste om lovgivningens mangler og tilpasser deres arbejdsmetoder for at holde sig klar af ulovlig virksomhed så længe som muligt.

Nogle myndigheder synes til tider tilbøjelige til at afholde sig fra håndhævelse på grundlag af strafferetten og tilskynder tjenesteudbydere til i første omgang at forsvare sig gennem civilretlige retsmidler i form af retssager. Selv om dette i visse tilfælde er acceptabelt, tilskynder en sådan politik ikke tjenesteudbyderne til at offentliggøre sager om piratvirksomhed, ligesom det kan berøve dem den

---

[52] Et typisk eksempel på en sådan fælles indsats er e-S.PA.C.E. Dublin 2001-projektet, der er gennemført under EU's Falcone-program, og hvor det irske politis *National Bureau of Criminal Investigation* og Microsoft sammen har udviklet en undervisningscd om piratvirksomhed og varemærkeforfalskning af software.

strafferetlige beskyttelse. Den gør dem sårbare over for modkrav om erstatning og negativ pr. Denne modvilje på begge sider bevirker, at der er mangel på pålidelige data om omfanget og typen af piratvirksomheden, hvilket yderligere komplicerer lovgivningen og håndhævelsen heraf.

Alle markedsaktører har anmodet om som minimum at få privat besiddelse og privat anvendelse af ulovlige anordninger med ind under definitionen på ulovlige handlinger. I de nordiske lande synes denne strategi at have været ganske effektiv til at holde piratvirksomheden nede.

En del respondenter, der ganske vist anerkendte forskellene i beskyttelsesomfanget, fremhævede lighedspunkterne i håndhævelsesforanstaltningerne, de procedurer, der skal følges, og de nationale retshåndhævende myndigheder, som beskæftiger sig med piratvirksomhed over for adgangsstyring, og de foranstaltninger, der vedrører hhv. varemærkeforfalskning og piratvirksomhed over for ophavsrettigheder.

Kommissionen opfordrer indtrængende medlemsstaterne og kandidatlandene til at skærpe håndhævelsen og yde udbydere af betalingstjenester en passende beskyttelse mod pirater, der opnår personlig vinding på udbydernes bekostning.

Kommissionen vil også fremover opfordre medlemsstaterne og kandidatlandene til at deltage i høringer om de resterende vanskeligheder ved håndhævelsen for at få kortlagt og bekæmpet lakunerne i lovgivningen.

Branchen og de retshåndhævende myndigheder bør fortsætte udviklingen af en fælles indsats for at komme piratvirksomheden til livs.

Kommissionen vil også fremover i videst muligt omfang yde støtte til denne udvikling både som led i sine støtteprogrammer, herunder rammeprogrammet om politisamarbejde og retligt samarbejde i kriminalsager (AGIS)[53], og de ressourcer, som er til rådighed, for at bistå kandidatlande med at øge deres administrative og retslige kapacitet.

4.4. Forretningspraksis, som ofte er udsat for piratvirksomhed

Kommissionen bliver med jævne mellemrum gjort opmærksom på, at nogle borgere ikke tillades adgang til beskyttede satellittv-udsendelser, der udsendes fra en anden medlemsstat end den, hvori de selv bor, selv om udsendelserne er lette at modtage mod en beskeden udgift via en parabolantenne[54], og selv om de er villige til at betale for en sådan adgang. Tjenesteudbydere indvender ofte, at de ikke har rettighederne for brugernes bopælsland, og at de skal anvende adgangsstyringsteknologier til at begrænse adgangen og beskytte ophavsretten. Borgerne kan ikke forstå, at de i det indre marked ikke kan få lovlig adgang til beskyttede betalingstv-tjenester, selv om de er rede til at betale abonnementsgebyrer og leveringsomkostninger.

---

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

54 Vedrørende "retten til at anvende en parabolantenne" har Kommissionen vedtaget en meddelelse om anvendelsen af det generelle princip om frie varebevægelser og fri udveksling af tjenesteydelser - EF-traktatens artikel 28 og 49, (KOM(2001) 351, endelig af 27.6.2001), http://europa.eu.int/comm/internal_market/en/media/satdish/index.htm.

Det er indlysende, at en sådan praksis udgør en stærk motivation for interesserede seere, f.eks. emigranter eller fagfolk og studerende med interesser for andre kulturer og samfund, til at omgå denne hindring og anvende ulovlige anordninger. Indtjeningen fra salget af disse ulovlige anordninger går til piraterne og ikke til tv-stationerne og rettighedshaverne. Normale modforanstaltninger til bekæmpelse af piratvirksomhed, der deaktiverer piratkort, reducerer ikke den udenlandske piratvirksomhed, fordi borgere, der ikke er bosiddende i tjenesternes hjemland, ikke lovligt kan købe gyldige smart cards og derfor må udøve piratvirksomhed, hvis de fortsat ønsker at kunne se nationalt fjernsyn. Disse forretningsmodeller stimulerer efterspørgselen efter ulovlige kort, skaber mulighed for piratvirksomhed, provokerer lovlydige borgere til at overtræde loven og hæmmer etableringen af det indre marked.

Afklaringen af rettigheder på en strengt national basis har også været genstand for arbejde i forbindelse med direktiv 93/83/EF om samordning af visse bestemmelser vedrørende ophavsrettigheder og ophavsretsbeslægtede rettigheder i forbindelse med radio- og tv-udsendelse via satellit og viderespredning pr. kabel[55]. Betalingstv-tjenester er blot den enkleste form for grænseoverskridende udbud af satellittv. Rettighedshavere forhandler de vilkår og betingelser, som er knyttet til udsendelsen af deres værker, med tv-stationerne. Betalingen står ofte i forhold til den forventede målgruppe. Teknologierne til adgangsstyring gør det muligt præcist at bestemme målgruppen uden for det oprindelige territorium (tjenesteudbyderen ved, hvem - nummer og adresse - der har købt hans kort) og opkræve gebyrer hos seerne (der har købt et kort). Adgangsstyring giver tv-stationerne mulighed for at betjene kunder uden for deres oprindelsesland og at yde kompensation til rettighedshaverne.

Forebyggende arbejde og en mere avanceret indsats for at neutralisere potentielle muligheder for piratvirksomhed fører ikke alene til en reel reduktion i piratvirksomheden, men gør også de ønsker, der er fremsat om en skærpet retlig beskyttelse mod de tilbageværende former for piratvirksomhed, mere troværdige.

Kommissionen har allerede offentliggjort, at den er i færd med at gennemgå de forskellige aspekter ved dette problem i et forsøg på - på gennemsigtig og afbalanceret vis - at forene de forskellige interesser, herunder rettighedshaveres ret til et rimeligt vederlag, satellittv-stationernes forretningspraksis og traktatens grundlæggende friheder[56].

Kommissionen opfordrer udbydere af elektroniske betalingstjenester til aktivt at søge måder at forhindre og reducere piratvirksomhed, for eksempel ved i samarbejde med rettighedshaverne at udvikle aftalebaserede løsninger, der giver legitime abonnenter uden for oprindelseslandet adgang til beskyttede elektroniske betalingstjenester på rimelige, ikke-diskriminerende og gennemsigtige vilkår, hvis sådanne tjenester af natur er tilgængelige i hele det indre marked.

---

55 EFT L 248 af 6.10.1993, s. 15, se også http://europa.eu.int/comm/internal_market/en/media/cabsat/dir/index.htm.

56 Kommissionens nylige rapport om satellitudsendelses- og kabel-videresprednings-direktivet 93/83/EF konkluderer, at friheden til at modtage og udsende tv-programmer fra andre medlemsstater, vil blive mindsket, hvis de vanskeligheder, der gør sig gældende ved overdragelse af ophavsrettigheder og beslægtede rettigheder, ikke bliver løst: KOM(2002) 430 endelig af 26.7.2002.

5. ANDEN JURIDISK UDVIKLING, DER PÅVIRKER UDBUDET AF ADGANGSSTYREDE OG ADGANGSSTYRENDE TJENESTER

5.1. Vedtagelse af direktiv 2001/29/EF om ophavsret og beslægtede rettigheder i informationssamfundet

Vedtagelsen i maj 2001 efter tre års indgående drøftelser af direktiv 2001/29/EF[57] var en milepæl i arbejdet på at lette grænseoverskridende handel med ophavsretsbeskyttede varer og tjenesteydelser. Direktivet, som for øjeblikket er under gennemførelse i medlemsstaterne, supplerer den retlige beskyttelse, som gives af direktivet om adgangsstyring, navnlig ved at yde retlig beskyttelse af antikopieringsanordninger og systemer til forvaltning af rettigheder. Det imødegår nogle af de bekymringer, som rettighedshavere har udtrykt med hensyn til manglen på beskyttelse i henhold til direktivet om adgangsstyring.

Uanset det nuværende anvendelsesområde for direktiv 2001/29/EF vil det på længere sigt være nødvendigt at tage hensyn til den seneste tekniske udvikling og de nyeste forretningsmodeller.

I begyndelsen beskyttede teknologier til adgangsstyring kun signalet, som det var spredt af tjenesteudbyderen. Den seneste generation af digitale hjemmenet og personlige videooptagere opretholder beskyttelsen i form af adgangsstyring i de efterfølgende stadier af det digitale forbrug.[58] Adgangsstyring har tendens til at indgå i større beskyttelsesarrangementer, der sigter på at tilvejebringe ende-til-ende-beskyttelse af indhold i alle processer fra den oprindelige distribution og frem til, at slutbrugeren ser og lytter til indholdet.[59] Adgangsstyring og forvaltning af digitale rettigheder kan benytte samme "krypterings-motor" i en husstands multimediecenter.[60]

Samtidig søger erhvervslivet nye måder at udnytte de tilgængelige teknologier til - på ofte uventet, innovativ vis - at tilbyde spændende indhold og optimere værdiskabelse og indtjening.[61] Disse nye forretningsmodeller er ofte eksperimenterende, i hvert fald i begyndelsen, og arbejder uden om den gældende retlige ramme.

Denne teknologiske konvergens vil ikke nødvendigvis og automatisk skulle føre til retlig konvergens, f.eks. samling af flere instrumenter til retlig beskyttelse i ét enkelt instrument.[62] Markedsudviklingen må imidlertid følges nøje for at sikre, at lovgivningen yder en helt sammenhængende og fuldstændig beskyttelse. Omvendt

---

57 EFT L 167 af 22.6.2001, s. 10.

58 Den nye generation af digitale videooptagere bruger ikke længere videobånd, men optager direkte på en harddisk, og de optagne programmer kan kun ses med et gyldigt smartcard.

59 Digital Video Broadcasting (DVB)-projektet arbejder for øjeblikket på at udvikle et nyt, integreret system til beskyttelse af indhold og styring af kopiering (Content Protection and Copy Management, CPCM) (www.dvb.org).

60 For yderligere baggrundsinformation og eksempler henvises til Kommissionens Arbejdsgruppes Dokument om Digitale Rettigheder, SEK(2002) 197 af 14.2.2002.

61 Nye online musiktjenester som Pressplay (en joint venture mellem Vivendi og Sony) er beskyttet af adgangsstyring, men omfatter også forvaltning af rettigheder til de downloadede eller streamede lydspor. En lignende udvikling findes inden for video on demand, hvor de mest populære film kan downloades via internet på abonnementsbasis med en styret efterfølgende visning, herunder med online realtids fornyelse af abonnementet efter den første visningsperiode.

62 Se endvidere fodnote 10.

skal overbeskyttelse undgås for ikke at hæmme innovation og økonomisk udvikling og undgå overdreven begrænsning af brugerrettigheder, herunder grundlæggende rettigheder som f.eks. ytringsfriheden eller retten til beskyttelse af privatlivets fred og til beskyttelse af personoplysninger.

På baggrund af denne juridiske, markedsmæssige og tekniske udvikling finder Kommissionen ikke, at tiden er inde til at foreslå at udvide den retlige beskyttelse, som direktivet giver mulighed for, til anvendelse af adgangsstyring af ophavsretlige årsager.

5.2. Vedtagelse af nye rammebestemmelser for elektroniske kommunikationstjenester

I marts 2002 blev Rådet og Europa-Parlamentet enige om et sæt direktiver og en afgørelse til fastlæggelse af de nye rammebestemmelser for elektroniske kommunikationstjenester og -net.[63] Denne lovpakke blev suppleret med et direktiv om databeskyttelse inden for elektronisk kommunikation, som blev vedtaget den 12. juli 2002.[64]

Denne lovpakke er en omfattende revision af den eksisterende EU-lovgivning om t0elekommunikation, som yderligere liberaliserer de berørte markeder og samtidig tilpasser regler til teknologisk konvergens. Den dækker elektroniske kommunikationsnet og -tjenester, herunder net og tjenester til radio-/tvspredning og tilknyttede faciliteter. Den specifikke lovgivning om systemer til adgangsstyring, som er fastlagt i direktiv 95/47/EF om anvendelsen af standarder for transmission af tv-signaler[65], revideres ligeledes.

Efter de nye rammebestemmelser for elektronisk kommunikation opfattes "adgangsstyringssystemer" som "tilhørende faciliteter".[66] Kravet om, at der skal tilbydes adgang til tjenester med adgangsstyring på ensartede, rimelige og ikke-diskriminerende vilkår, og kravene om interoperabilitet for adgangsstyring, som første gang blev fastlagt i direktiv 95/47/EF[67], er blevet videreført til de nye rammebestemmelser, idet de dog vil blive gjort til genstand for ændringer.[68] Navnlig er styret adgang til digitale radiotjenester nu omfattet, og der er indført markedsanalyseprocedurer til gennemgang af forpligtelser i forbindelse med styret adgang til digitale udsendelser, hvilket især indebærer, at medlemsstaterne på visse betingelser kan ændre eller tilbagetrække adgangsbetingelser for udbydere, som ikke

---

63 IP/02/259 af 14.2.2002, direktiv 2002/19/EF (adgangsdirektivet), direktiv 2002/20/EF (tilladelses-direktivet), direktiv 2002/21/EF (rammedirektivet), direktiv 2002/22/EF (forsyningspligtdirektivet), beslutning 676/2002/EF (frekvenspolitikbeslutningen), EFT L 108 af 24.4.2002.

64 Direktiv 2002/58/EF, EFT L 201 af 31.7.2002.

65 EFT L 281 af 23.11.1995, s. 51 (ophævet pr. 25.7.2003), http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm.

66 Direktiv 2002/21/EF, EFT L 108 af 24.4.2002, s. 33, artikel 2, litra e) og f).

67 Direktiv 95/47/EF gav bl.a. mulighed for anvendelse af Common Scrambling Algorithm, som forvaltes af ETSI (denne algoritme angiver, hvordan dekrypteringsfunktionen i en dekoderboks deciffrerer den beskyttede udsendelse), muligheden for at modtage frit-i-luften transmissioner samt DVB Common Interface connector (dette er en standardiseret grænseflade mellem et udskifteligt tilslutningsmodul til adgangsstyring og dekoderboksen, der giver mulighed for, at flere forskellige teknologier til adgangsstyring kan bruges på samme boks).

68 Direktiv 2002/22/EF, EFT L 108 af 24.4.2002, s. 51, artikel 24 og bilag VI.

har en stærk markedsposition.[69] Systemer til og tjenester med adgangsstyring er ikke omfattet af tilladelsesdirektivet.[70]

Selv om disse konkurrencefremmende rammebestemmelser ikke yder retlig beskyttelse mod piratvirksomhed over for adgangsstyrede og adgangsstyrende tjenester, styrer det tilvejebringelsen af elektroniske kommunikationsnet og -tjenester i almindelighed og adgangsstyrede og adgangsstyrende systemer i særdeleshed og er som sådan meget vigtigt for den videre udvikling af markedet i de kommende år.

Kommissionen vil nøje se på den fremtidige udvikling på markederne for adgangsstyring efter de nye rammebestemmelser for elektronisk kommunikation, når den skal fastslå, om der er behov for yderligere foranstaltninger til bekæmpelse af piratvirksomhed.

5.3. Gennemførelse af direktiv 2000/31/EF om elektronisk handel

Selv om definitionen af informationssamfundets tjenester har eksisteret i fællesskabslovgivningen helt fra vedtagelsen af direktiv 98/48/EF[71], er det først med vedtagelsen af e-handelsdirektivet[72], at medlemsstaterne er blevet pålagt at indføre et omfattende sæt love og administrative bestemmelser om informationssamfundets tjenester.

Gennemførelsen af e-handelsdirektivet vil øge retssikkerheden for erhvervslivet og forbrugerne og have en positiv effekt på en hurtig udvikling af alle former for nye interaktive tjenester over internet, herunder tjenester, som er beskyttet med adgangsstyring og udbydes mod vederlag.

Med gennemførelsen af direktivet om adgangsstyring har de fleste medlemsstater allerede indført begrebet "informationssamfundets tjenester" i deres retssystemer. For at opretholde retssikkerheden bør medlemsstaterne ikke indføre anderledes eller modstridende definitioner i deres nationale lovgivning.

E-handelsdirektivet fastsætter bl.a. et sæt fælles regler, der begrænser formidleransvaret hos visse tjenesteydere, herunder udbydere af hostingtjenester[73]. Disse regler dækker ansvaret for alle former for ulovlig virksomhed, der iværksættes online af tredjemand, herunder udbredelsen af information med relation til piratvirksomhed, eller endda ulovlige anordninger via websteder, nyhedsgrupper og elektroniske opslagstavler.[74]

---

69 Direktiv 2002/19/EF, EFT L 108 af 24.4.2002, s. 7, artikel 2, litra a), artikel 6 og bilag I.

70 Direktiv 2002/20/EF, EFT L 108 af 24.4.2002, s. 21, betragtning 6.

71 Europa-Parlamentets og Rådets direktiv 98/48/EF af 20. juli 1998 om ændring af direktiv 98/34/EF om en informationsprocedure med hensyn til tekniske standarder og forskrifter, EFT L 217 af 5.8.1998, s. 18.

72 Direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (direktivet om elektronisk handel), EFT L 178 af 17.7.2000, s. 1-16.

73 Artikel 14, stk. 1, i e-handelsdirektivet fritager formidlere, der oplagrer offentligt tilgængelig information, som er leveret af deres kunder (såkaldt hosting), for erstatningsansvar for den oplagrede information, hvis forskellige betingelser er opfyldt.

74 Af særlig vigtighed er procedurerne til "fjernelse af ulovligt indhold", når det er kommet til den pågældende ISP's "kendskab", at materialet kan være ulovligt. Direktivet om e-handel regulerer ikke disse procedurer vedrørende "fjernelse af ulovligt indhold", men skaber rammerne for udvikling af selvregulerende løsninger.

Kommissionen vil påse, at eventuelle yderligere initiativer om adgangsstyring er i overensstemmelse med e-handelsdirektivet.

5.4. Forslaget om Rådets rammeafgørelse om angreb mod informationssystemer

Kommissionen vedtog for nylig et forslag til Rådets rammeafgørelse om angreb på informationssystemer.[75] Dette forslag søger at tilnærme strafferetten i hele EU for at sikre, at de retshåndhævende og retslige myndigheder i Europa kan tage affære over for de nye og alvorligste former for kriminelle handlinger mod informationssystemer og sigter mod at supplere det, som allerede er opnået inden for fællesskabsretten, for så vidt angår beskyttelse af informationssystemer, uden i øvrigt at berøre fællesskabsretten.[76]

Den foreslåede rammeafgørelse dækker bl.a. uautoriseret adgang til en computer eller til computernetværk, herunder adgang til tjenester, som er beskyttet af adgangsstyring uden vederlag. Det erkendes i forslaget, at adgangsstyrende anordninger, herunder digitale dekoderbokse og personlige videooptagere, er "computere", og at tjenester, som er beskyttet af adgangsstyring, leveres via et "informationssystem".

Hvis Rådet fastholder den model, Kommissionen har foreslået, vil medlemsstaterne skulle træffe passende foranstaltninger til at gøre det til en lovovertrædelse at opnå ulovlig adgang til informationssystemer, hvis dette sker mod et informationssystem, der er underlagt specifikke beskyttelsesforanstaltninger (f.eks. en betalingstv-tjeneste, der anvender adgangsstyring) eller med den hensigt at forvolde skade (f.eks. mod udbyderen af teknologien til eller tjenesten med adgangsstyring) eller opnå en økonomisk fordel (f.eks. ved at opnå fortjeneste ved at sælge ulovlige anordninger).[77] I forslaget sondres der ikke mellem at udføre denne kriminelle handling i privat eller kommercielt øjemed, ej heller kræver det, at den pågældende tjeneste udbydes mod vederlag. Det er heller ikke efter forslaget et krav, at systemerne til adgangsstyring i alle tilfælde skal være omgået, for at der er tale om en lovovertrædelse.

Forslaget til rammeafgørelse supplerer den retlige beskyttelse, som ydes af direktivet om adgangsstyring, og sikrer et yderligere beskyttelsesniveau mod piratvirksomhed mod betalingstjenester, som er beskyttet med adgangsstyring.

6. BEKÆMPELSE AF PIRATVIRKSOMHED - EN TVÆREUROPÆISK INDSATS

6.1. Henstilling nr. R (91) 14 om retlig beskyttelse af krypterede fjernsynsprogrammer

Helt tilbage i september 1991 vedtog Europarådet en henstilling om retlig beskyttelse af krypterede fjernsynsprogrammer.[78] Denne henstilling har været inspirationskilde

---

75 KOM(2002) 173 endelig af 19.4.2002.

76 Se navnlig EU-traktatens artikel 47, betragtning18 i udkast til rammeafgørelse og KOM(2002) 173, punkt 1.6.

77 Udkast til rammeafgørelse, artikel 3.

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

for lovgivere i mange europæiske lande.[79] Den har dannet overgang til både fællesskabsdirektivet og dets modstykke, den europæiske konvention om adgangsstyring, European Conditional Access Convention.

Henstillingen er den første generation af retlig beskyttelse. Den beskytter udelukkende fjernsynsprogrammer, der anvender krypteringsteknikker, og sondrer ikke mellem betalingstjenester og gratistjenester eller mellem forskellige årsager til anvendelse af kryptering.

Interessant nok hedder det i henstillingen, at udbydere af krypterede fjernsynsprogrammer har ansvaret for at anvende de bedste krypteringsteknikker, som er tilgængelige.

Ifølge henstillingen opfattes alle kommercielle og private aktiviteter vedrørende fremstilling, import, distribution og kommerciel reklame for dekodere, der giver adgang uden for den af tjenesteudbyderen fastlagte målgruppe, som ulovlige. Besiddelse i kommercielt øjemed betragtes ligeledes som ulovlig, mens vurdering af ulovligheden af privat besiddelse overlades til de enkelte medlemsstater.

I henstillingen understreges behovet for hensigtsmæssige straffesanktioner og administrative sanktioner samt tab af rettigheder til beslaglagte dekodere og økonomisk gevinst, erhvervet ved de ulovlige aktiviteter.

Tiden har vist, at Europarådets pionerindsats for at supplere den tekniske beskyttelse med retlig beskyttelse har haft afgørende indvirkning på opbygningen af konsensus blandt de europæiske lande om, hvordan piratvirksomhed kan håndteres effektivt.

6.2. Den europæiske konvention ETS nr. 178 om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester

Som reaktion på piratvirksomhedens stigende omfang gik Europarådets medlemsstater videre - parallelt med vedtagelsen af direktivet - til forhandlinger om et tilsvarende, bindende instrument. Kommissionen forhandlede denne konvention på Fællesskabets og dets medlemsstaters vegne på baggrund af Rådets mandat af 12. juni 1999.

Under forhandlingerne om konventionen har Kommissionen været særlig opmærksom på at holde direktivet og konventionen så tæt tilpasset hinanden som muligt. Konventionen omfatter i det store og hele de samme områder som direktivet, og det er udtrykkeligt fastsat, at Det Europæiske Fællesskab kan tiltræde den.

Efter at konventionen blev åbnet for undertegnelse den 24. januar 2001, er den blevet undertegnet af tre EU-medlemsstater og af tre kandidatlande[80]. Indtil videre har Cypern og Rumænien formelt ratificeret konventionen. En række andre kandidatlande har tilkendegivet deres hensigt om at tiltræde konventionen. Det er fastlagt i konventionen, at tre stater skal tiltræde den, før den kan træde i kraft.

---

79 På baggrund af denne henstilling er der blevet indført lovgivning til beskyttelse af krypterede fjernsynsprogrammer i starten af halvfemserne af en række lande, herunder Danmark, Finland, Frankrig, Irland, Nederlandene og Det Forenede Kongerige.

80 Konventionens fulde tekst, begrundelsen og de seneste oplysninger vedrørende undertegnelse og ratifikation findes på http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=178&CM=8&DF=.

For at tilvejebringe en sammenhængende, tværeuropæisk retlig ramme og et ensartet beskyttelsesniveau mod piratvirksomhed i hele Europa er det vigtigt, at Europarådets konvention nr. 178 træder i kraft snarest muligt. Kommissionen vil arbejde hen imod en ratificering af konventionen.

6.3. Den juridiske situation i de øvrige europæiske lande

I henhold til bestemmelserne i Aftalen om Det Europæiske Økonomiske Samarbejdsområde besluttede Det Blandede EØS-udvalg den 28. februar 2001[81] at indarbejde direktivet i aftalens bilag X og XI. Denne beslutning trådte i kraft den 1. oktober 2001; den praktiske gennemførelse reguleres af EØS' regler og procedurer. Ud af de tre deltagende tredjelande er det kun Liechtenstein, der endnu ikke har vedtaget nogen gennemførelseslovgivning. Norge har undertegnet Europarådets konvention nr. 178 og har ændret norsk straffelov i overensstemmelse hermed.[82] Island har ændret sin medielovgivning.[83]

Schweiz har undertegnet Europarådets konvention nr. 178 og er i færd med at forberede den formelle ratificering og gennemførelsen i national ret.

San Marino, Monaco og Andorra har ingen specifik lovgivning på direktivets område. Manglen på hensigtsmæssig lovgivning kan resultere i lakuner i den tværeuropæiske beskyttelse mod piratvirksomhed og risiko for underminering af den retlige beskyttelse ved at skabe fristeder for pirater.

Kommissionen opfordrer de lande, som ikke bliver medlemmer af det udvidede EU, til at tilslutte sig Fællesskabets indsats for et ensartet beskyttelsesniveau mod piratvirksomhed i hele Europa.

6.4. Den europæiske konvention ETS nr. 185 om cyberkriminalitet

Med henblik på at videreføre den fælles kamp mod cyberkriminalitet har Europarådet forberedt en konvention om cyberkriminalitet, som har været åben for undertegnelse siden den 23. november 2001.[84] Indtil datoen for denne rapport er denne konvention undertegnet af 13 EU-medlemsstater og flere kandidatlande samt visse andre stater.

Konventionen pålægger de stater, der tiltræder konventionen, at gøre bl.a. ulovlig adgang (hacking) til informationssystemer og, hvad der er vigtigere, misbrug af anordninger, til en kriminel handling i henhold til national ret. Bestemmelserne vedrørende misbrug af anordninger, som fastlagt i konventionens artikel 6, forbyder de traditionelle aktiviteter (f.eks. fremstilling, salg, distribution og besiddelse) i relation til sådanne anordninger samt computer-passwords og adgangskoder og er af særlig interesse på grund af deres omfang og generelle art samt deres potentiale for at standse internet-relateret piratvirksomhed.

Ikke-europæiske landes deltagelse rummer løfter om globale løsninger, hvilket er særlig vigtigt for bekæmpelse af internet-relaterede ulovlige handlinger. Et

---

81 Afgørelse nr. 17/2001 af 28.2.2001, EFT L 117 af 26.4.2001, s. 21.

82 Norsk strafferet, artikel 262, som har været i kraft siden 1.8.2001.

83 Radiospredningslov nr. 53 af 17.5.2000.

84 Konventionens fulde tekst, begrundelsen og de seneste oplysninger vedrørende undertegnelse og ratifikation findes på http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=.

transatlantisk samarbejde vedrørende gennemførelse og håndhævelse af konventionens piratvirksomhedsbekæmpende bestemmelser i relation til adgangsstyring bør undersøges yderligere og om muligt udvides til andre fora.

Selv om EU ikke kan tiltræde konventionen, bør dens løsninger inden for forhold med relation til adgangsstyring tages i betragtning og eventuelt anvendes som model for yderligere udvikling af piratvirksomhedsbekæmpende foranstaltninger i EU.

7. ENDELIGE KONKLUSIONER OG DET VIDERE ARBEJDE

7.1. Elektroniske betalingstjenester er vigtige for en videnbaseret økonomi i fuld udvikling

I dag findes elektroniske betalingstjenester navnlig inden for digitalt betalingstv. En massiv udbredelse af alle mulige former for nye elektroniske betalingstjenester, som udbydes over alle mulige distributionsnet, ventes i almindelighed at ske i dette årti. De første eksempler på abonnementsbaserede informationssamfundstjenester, der leverer særligt populært indhold over internet, har for nylig vist sig. Digitaliseringen af kabelnettene samt indførelsen af digitalt landbaseret tv, 3G-mobilkommunikation og avancerede transportrelaterede tjenester vil i en ikke alt for fjern fremtid føre til en storstilet udbredelse af intelligente apparater, der kan håndtere betalingstjenester. Nye former for forbrugerelektronik såsom integrerede hjemmeunderholdningscentre og personlige videooptagere vil blive designet til at give større lytter- og seeroplevelser, selv om der anvendes teknologier til adgangsstyring, og selv om fuld adgang kun er mulig mod betaling.

Det 21. århundredes videnbaserede økonomier ventes i stadigt stigende omfang at blive afhængige af påtrængende elektroniske betalingstjenester. Derfor vil den økonomiske og samfundsmæssige betydning af disse tjenester vokse med tiden. Bedrageri og piratvirksomhed med relation til betalingstjenester vil have tendens til at udvikle sig med samme hastighed som selve betalingstjenesterne, medmindre man sikrer tilstrækkelig retlig beskyttelse og effektiv håndhævelse. Piratvirksomhed mod elektroniske betalingstjenester har samme skadelige virkninger i informationssamfundet som økonomisk kriminalitet og vareforfalskninger havde i det tyvende århundrede. Der skal tages hensyn til denne udvikling, hvis EU vil opfylde sit ambitiøse mål om at blive den mest dynamiske og konkurrencedygtige økonomi i verden i 2010.[85]

Det er derfor vigtigt at sende et klart signal til erhvervsliv og borgere om, at EU og dens medlemsstater ikke kan acceptere, at den økonomiske og samfundsmæssige udvikling i EU hæmmes alvorligt af piratvirksomhed, hvorfor der i offentlighedens interesse må gribes ind. Et tidligt og tydeligt signal kan forhindre udvikling af tolereret og socialt accepteret piratvirksomhed på et niveau, som for øjeblikket kendes på området for digital musik.

---

[85] Det Europæiske Råd i Lissabon, den 23.-24. marts 2000, formandsskabets konklusioner, afsnit 5.

Kommissionen opfatter elektroniske betalingstjenester som et centralt omdrejningspunkt for den nye videnbaserede økonomi. Retlig beskyttelse mod piratvirksomhed over for elektroniske betalingstjenester udgør en væsentlig betingelse for udviklingen af sådanne tjenester og en forudsætning for fremtidig vækst og velstand for EU's borgere.

7.2. Konsolidering af den nuværende retlige beskyttelse - fremtidige foranstaltninger

Direktivet sikrer allerede i sin nuværende form en betydelig retlig beskyttelse mod piratvirksomhed over for elektroniske betalingstjenester, som er beskyttet med adgangsstyring. Som det fremgår af denne rapport, er der fortsat plads til forbedringer af den nuværende retlige beskyttelse uden at ændre selve direktivet.

Direktivet er endnu ikke fuldt gennemført i det udvidede EU, og håndhævelsen på nationalt plan skal konsolideres. Industrien og de retshåndhævende myndigheder skal fortsat udvikle deres offentlige/private partnerskaber i en fælles indsats mod piratvirksomhed, eventuelt med støtte fra EU's ressourcer.

En vellykket bekæmpelse af piratvirksomhed indbefatter også aktive forebyggende foranstaltninger og en offensiv indsats for at reducere gråzoner, hvor piratvirksomheden kan blomstre. Adgang til beskyttet satellitbaseret betalingstv for betalende seere uden for udsendelsernes oprindelsesland bør gøres mulig.

Det vil kun være muligt at bekæmpe piratvirksomheden effektivt, hvis piraterne ikke kan finde fristeder i Europa. En hurtig ikrafttrædelse af Europarådets konvention nr. 178 vil bidrage væsentligt til at nå dette mål.

Sammenfattende kan der træffes følgende foranstaltninger for at styrke direktivets virkning:

- Kommissionen vil arbejde ihærdigt på at sikre fuld gennemførelse af direktivet. Den vil samarbejde med medlemsstaterne og kandidatlandene om fuld gennemførelse af direktivet og afklare alle resterende retlige tvivlsspørgsmål. Kommissionen vil efter behov indlede traktatbrudsprocedurer.

- Kommissionen vil høre medlemsstaterne om de praktiske vanskeligheder, de kommer ud for ved håndhævelsen af de nationale bestemmelser, der gennemfører direktivet.

- Kommissionen vil tilskynde branchen og de nationale myndigheder til en fælles indsats for at bekæmpe piratvirksomhed så virkningsfuldt og effektivt som muligt.

- Kommissionen vil fortsat samarbejde med andre europæiske lande og relevante internationale organisationer om at sikre en sammenhængende anvendelse af europæiske regler mod piratvirksomhed over for elektroniske betalingstjenester.

- Kommissionen anbefaler rettighedshavere og tjenesteudbydere aktivt at søge aftalebaserede løsninger for at tilbyde legitime abonnenter uden for tjenesternes oprindelsesland adgang til beskyttede elektroniske betalingstjenester på rimelige, ikke-diskriminerende og gennemsigtige vilkår i hele det indre marked. Kommissionen vil bidrage til denne proces ved revisionen af direktiv 93/83/EF.

7.3. Forbedring af den retlige beskyttelse - hvad bringer fremtiden?

Piratvirksomhed over for elektroniske betalingstjenester, der er beskyttet med adgangsstyring, er en form for cyberkriminalitet, der har ændret sig markant i de senere år. Selv om den nuværende retlige beskyttelse er ganske effektiv over for de traditionelle former for piratvirksomhed, kan det være nødvendigt at forbedre beskyttelsen for at klare de nye kategorier af lovovertrædere, internettets konsekvenser og en række tilbageværende håndhævelsesproblematikker.

På baggrund af det skønnede potentiale for beskyttelse gennem supplerende aktioner, der baseres på det gældende direktiv, er det Kommissionens opfattelse, at det er for tidligt at foreslå ændringer af direktivet i lyset af denne rapport, men også at en revision af direktivet muligvis bør overvejes i forbindelse med et sammenhængende sæt retlige foranstaltninger mod alle mulige former for piratvirksomhed.

De høringer og vurderinger, som er gennemført i forbindelse med udarbejdelsen af denne rapport, har imidlertid allerede gjort det muligt for Kommissionen at afdække følgende problemstillinger, som fortjener nærmere overvejelse i nært samarbejde med medlemsstaterne og branchen:

- Industrielle former for piratvirksomhed er klart kommercielle og er derfor allerede omfattet af direktivet om adgangsstyring. Denne type piratvirksomhed ligner meget forfalskning af varer eller piratvirksomhed med relation til ophavsrettigheder. En balanceret og sammenhængende ramme for håndhævelsen, som kan finde anvendelse på alle former for piratvirksomhed og forfalskninger, og som vedtages på EU-plan, vil kunne øge effektiviteten af den retlige beskyttelse af elektroniske betalingstjenester.
- Der har været fremført argumenter om, at fritidspirater og enkeltpersoner, der alene udfører piratvirksomhed til egen gavn, kan retsforfølges, herunder for ulovlige handlinger, der ikke udføres i kommercielt øjemed, og/eller for privat besiddelse af ulovlige anordninger. En udvidelse af direktivet om adgangsstyring i denne forstand ville imidlertid indebære en grundlæggende ændring i EU's politik og kan have indvirkning på tilstødende lovgivning.
- Det nuværende direktiv er ikke særlig effektivt mod de former for piratvirksomhed, som har udviklet sig på grund af internet. En måde at bekæmpe disse former for piratvirksomhed på er ved at forbyde den direkte og indirekte distribution af nøgler og ulovlige anordninger via internet, suppleret med et retsmiddel vedrørende varsling om og fjernelse af ulovligt materiale for berørte tjenesteudbydere. Sådanne forbud/retsmidler er rettet mod den primære kilde til mange former for piratvirksomhed og kan bidrage til at undgå andre foranstaltninger, der kan være mere indgribende over for enkeltpersoner. Artikel 6 i Europarådets konvention om cyberkriminalitet indeholder i forvejen en model for en sådan foranstaltning. I denne sammenhæng påtænker Kommissionen ikke at træffe nogen foranstaltninger, der indskrænker udbredelsen af detaljeret teknisk information om adgangsstyringssystemer, da dette i urimelig grad ville hindre ytringsfriheden og hæmme innovationen.

Kommissionen vil også fremover se på anvendelsen af direktivet om adgangsstyring og forholdet mellem direktivet og de øvrige bestemmelser i fællesskabsretten, herunder hvorvidt der er behov for at ændre direktivet. Den opfordrer medlemsstaterne, kandidatlandene og andre berørte parter til at bidrage hertil.