

KÄRANDE

STOP, Scandinavian TV Organisations against Piracy –
Sweden AB,
Skårs led 3 B, 412 63 GÖTEBORG
Ombud: advokaten Thomas Carlén-Wendels,
Advokatfirman Konsultbyrå för Marknadsrätt AB,
Kungsgatan 48, 111 35 STOCKHOLM

SVARANDE

1. KeyCard.dk I/S, Rømersgade 25,
1362 KÖPENHAMN, Danmark
2. I. F.
Ombud för 1-2: advokaten Michael Lettius och jur. kand.
Carl-Johan Ask, Advokatfirman Glimstedt, Box 1027,
251 10 HELSINGBORG

SAKEN

marknadsföring av avkodningsutrustning

DOMSLUT

1. Marknadsdomstolen förbjuder KeyCard.dk I/S vid vite av fyrahundratusen (400 000) kr att i Sverige marknadsföra sådana kort och programmerare som framgår av domsbilagan eller andra sådana kort och programmerare som utgör avkodningsutrustning som enligt lag inte får överlåtas.
2. Marknadsdomstolen lämnar STOP:s yrkande mot I. F. utan bifall.

3. KeyCard.dk I/S skall ersätta STOP, Scandinavian TV Organisations against Piracy – Sweden AB dess rättegångskostnader med trehundrasjuttioåttatusenniohundrafemtioåtta (378 958) kr jämte ränta enligt 6 § räntelagen (1975:635) från dagen för Marknadsdomstolens dom till dess betalning sker. Av beloppet avser 303 600 kr ombudsarvode.
4. STOP, Scandinavian TV Organisations against Piracy – Sweden AB skall ersätta I. F. dennes rättegångskostnader med femhundraniotusenåttahundratjugotre (509 823) kr jämte ränta enligt 6 § räntelagen (1975:635) från dagen för Marknadsdomstolens dom till dess betalning sker. Av beloppet avser 358 000 kr ombudsarvode.
5. Marknadsdomstolen förordnar att sekretess enligt 8 kap. 17 § sekretesslagen (1980:100) skall bestå beträffande upptagningen av förhöret med R. P. (band 1 s. B 16,6 – 30,9) och KeyCard.dk I/S och I. F:s slutanförande i de delar dessa ägt rum inom stängda dörrar samt den bild, aktbilaga 112 s. 5, som förevisats inom stängda dörrar avseende uppgifter om ett låssystem som är under utveckling.

YRKANDEN M.M.

STOP, Scandinavian TV Organisations against Piracy – Sweden AB (STOP) har, som dess talan slutligen bestämts, yrkat att KeyCard.dk I/S (KeyCard) och I. F. var för sig vid vite skall förbjudas att i Sverige eller från Sverige marknadsföra sådan avkodningsutrustning som inte får yrkesmässigt marknadsföras eller överlåtas här i landet. Om Marknadsdomstolen skulle finna att de aktuella programmerarna inte kan betraktas som avkodningsutrustning, har STOP yrkat att marknadsföring av dessa programmerare likväl skall förbjudas då marknadsföringen är otillbörlig och strider mot god marknadsföringssed.

I. F. har för egen del i första hand yrkat att STOP:s talan mot honom skall avvisas. I andra hand har han gemensamt med KeyCard bestritt STOP:s talan. De har vidare anfört, för det fall Marknadsdomstolen skulle meddela ett förbud i målet, att ett sådant förbud bör inskränkas till att avse försäljning till köpare som inte intygar att produkterna inte kommer att användas till otillåten avkodning. I. F. och KeyCard har, som det får uppfattas, också yrkat att STOP:s andrahandsyrkande under alla förhållanden skall avvisas då yrkandet måste anses utgöra en otillåten taleändring.

STOP har bestritt samtliga avvísingsyrkanden och yrkandet om att ett förbud skall inskränkas på av KeyCard och I. F. angivet sätt.

Parterna har yrkat ersättning för sina rättegångskostnader.

Marknadsdomstolen har i beslut den 26 augusti 2003 ogillat ett av KeyCard och I. F. framställt yrkande om avvísning av STOP:s talan på grund av att marknadsföringslagen (1995:450) (MFL) inte skulle vara tillämplig och Marknadsdomstolen inte behörig att handlägga målet.

Marknadsdomstolen har vidare i beslut den 14 april 2004 ogillat av STOP framställda yrkanden om syn och edition samt en framställan av KeyCard och I. F. att inhämta förhandsavgörande från EG-domstolen.

GRUNDER OCH UTVECKLING AV TALAN

Bakgrund

STOP är ett av TV-industrin gemensamt bildat bolag med uppgift att skydda kodade tjänster från obehörig tillgång genom att bevaka och beivra olaglig hantering av olovlig avkodningsutrustning.

KeyCard är ett danskt handelsbolag, ett intresseselskab (I/S), som har säte i Köpenhamn. Företaget har varit verksamt sedan år 1998. Företaget verkar inom teknik- och elektronikbranschen och bedriver bl.a. e-handel via sin webbsida.

Betal-TV bygger på abonnemang, till skillnad från licens- och reklamfinansierade TV-sändningar. För att utestänga andra än abonnenter sker därför sändningarna i krypterad form och det krävs en avkodningsutrustning för att kunna se dem. Endast abonnenter med auktoriserad avkodningsutrustning är behöriga att ta del av det kodade programinnehållet. Avkodningsutrustningen – som numera genomgående består av s.k. smarta kort – tillhandahålls som en del av abonnemanget och får brukas av abonnenten under avtalstiden. Abonnenten är genom avtalsvillkor alltid förbjuden att överlåta eller på annat vis fränhända sig avkodningskortet. Kortet används tillsammans med kabel- och satellitmottagare som antingen tillhandahålls av respektive TV-operatör som del av ett abonnemang eller som fri handelsvara på

marknaden. Dessa mottagare innehåller i sig ingen avkodningsförmåga utan denna funktion ligger helt i kortet.

Vid sidan av de avkodningskort som tillhandahålls genom abonnemang förekommer även en stor illegal marknad för handel med s.k. piratkort. Enligt lagen (2000:171) om förbud beträffande viss avkodningsutrustning (dekoderlagen) är det straffbart att i förvärvssyfte olovligen hantera avkodningsutrustning i avsikt att bereda någon utanför abonnentkretsen tillgång till innehållet i en kodad sändning.

De s.k. piratkorten förekommer på marknaden dels i form av färdigprogrammerade kort med programvara och aktuella krypteringsnycklar, dels som kort med tomma program- och minneskretsar. Till de tomma korten hämtas programvara och krypteringsnycklar hem av kunden själv över Internet och överförs till det tomma kortet med hjälp av en liten kortläsare/skrivare ("programmerare" eller "brännare") som ansluts till en dator. Marknadsdomstolen har i tidigare avgöranden funnit vissa tomma kort utgöra olovlig avkodningsutrustning och meddelat förbud för fortsatt marknadsföring av sådana kort (MD 2002:15 och 2002:16).

De av KeyCard saluförda tomma korten och programmerarna kan, sedan programvara därför har hämtats hem från Internet, användas till att olovligen avkoda TV-sändningar.

STOP har i målet gjort gällande att samtliga av KeyCard marknadsförda kort och programmerare, vilka framgår av exempelvis domsbilagan, saknar annat reellt användningsområde än att avkoda TV-sändningar samt att de påtalade programmerarna under alla förhållanden utgör en nödvändig beståndsdel i den otillåtna utrustningen.

KeyCard och I. F. har gjort gällande att företaget inte bedriver marknadsföring i Sverige, att det skulle strida mot EG-rätten att meddela förbud i enlighet med STOP:s yrkande samt att de aktuella produkterna har ett stort antal legala användningsområden, varför de inte kan anses utgöra otillåten avkodningsutrustning.

Parterna har härutöver utvecklat sin talan enligt följande.

STOP

Samtliga av KeyCard marknadsförda kort och programmerare, vilka framgår av domsbilagan, saknar annat reellt användningsområde än att avkoda TV-sändningar och utgör därmed otillåten avkodningsutrustning. KeyCards marknadsföring skall därför anses otillbörlig och stridande mot god marknadsföringssed i enlighet med den s.k. lagstridighetsprincipen. Under alla förhållanden har de påtalade programmerarna inte något annat användningsområde än att användas tillsammans med otillåten avkodningsutrustning (piratkort). Programmerarna utgör en nödvändig beståndsdel i den otillåtna utrustningen och har ingen annan praktisk funktion än att förse korten med program för TV-avkodning och marknadsföringen av dessa är därför under alla förhållanden otillbörlig och strider mot god marknadsföringssed.

KeyCard och dess verksamhet

När KeyCard startade sin verksamhet hette bolaget DK2Mac och sålde programmerade piratkort. På den tiden kallades piratkort allmänt för "D2Mac-kort" efter det förhärskande sändningssystemet för analog satellit-TV i Skandinavien, D2Mac. Sedan DK2Mac och dess innehavare åren 1999 och 2000 förbjudits att marknadsföra piratkort och programmerare bytte bolaget namn till KeyCard och började sälja tomma kort och programmerare till dessa. KeyCard bedriver idag en omfattande verksamhet. KeyCards försäljning sker från såväl Danmark som Sverige. Försäljningen sker lokalt från butik på Rømersgade i Köpenhamn och via postorder från webbplatser på Internet. Den svenska mycket omfattande verksamheten är förlagd till Vejbystrand i Skåne.

KeyCard är sedan flera år en av de största leverantörerna av piratkort i Skandinavien med försäljning till såväl enskilda konsumenter som vidare distributörer. Marknadsprofilen är genomgående och uteslutande förknippad med TV-avkodning. KeyCard förekommer med annonsering och annan närvaro i praktiskt taget alla sammanhang med anknytning till olovlig avkodning. På webbplatsen "www.satinfo.org", en av de mer välkända piratmanualerna på nätet med omfattande information om hur avkodningsutrustning fungerar och används, annonserar KeyCard på ett flertal sidor med i vart fall tre olika 8- respektive 18-sidiga bannerannonser. Enligt sökmotorn, statistikinsamlaren och statistiksäljaren Chart.dk har KeyCards webbplats en hög besöksfrekvens och annonserar där sina kort och programmerare under avdelningen för satellit-mottagnings-tillbehör. KeyCard presenterar sig där som "Skandinaviens största säljare av brännare och kort".

Företagets webbplats finns i en dansk, en engelsk och en svensk version. I KeyCards svenska version av webbplatsen uppges bolagets svenska fysiska adress i Vejbystrand samt svenska telefon- och faxnummer för beställning och support med telefontider m.m. samt en särskild svensk e-adress hos Telia. KeyCard har också svenska post- och bankgironummer för betalningar från Sverige eller från svenska kunder. KeyCard är momsregistrerat i Sverige och har ett svenskt momsregistreringsnummer. Fakturering av svenska kunder sker från Sverige, med svenska fakturor och med svenska adresser och andra fiskalt obligatoriska uppgifter. På den svenska webbplatsen uppges att "Alla order sänds från Sverige". Betalning från Sverige sker också till KeyCard i Sverige. På webbplatsen anges att "Samtidigt vill vi göra dig uppmärksam på att du som kund hos oss naturligtvis är 100 % anonym och att vi under inga omständigheter lämnar några uppgifter om dina köp till några myndigheter, men kom ihåg att det är DITT ansvar vad du väljer att använda våra produkter till".

Vid en husrannsakan hos en av Skandinaviens större – men inte ende – grossister som distribuerar piratkort har påträffats fakturor utställda på KeyCard Sverige avseende leveranser av piratkort av olika typer. Av fakturorna framgår att KeyCard vid 32 tillfällen under tiden januari till oktober år 2002 har inhandlat totalt 78 737 st piratkort från denna grossist. Dessa 32 fakturor avser uteslutande KeyCard Sverige och samtliga leveranser har skett från grossisten med transportföretaget DHL direkt till Vejbystrand. STOP förutsätter att KeyCard Sverige säljer kort i samma utsträckning som de köps in. STOP beräknar att KeyCard Sverige omsätter omkring en miljon kronor på kort varje månad med en vinstmarginal på uppskattningsvis 50 %.

Den påtalade marknadsföringen

Den påtalade marknadsföringen av otillåtna avkodningskort och programmerare framgår bl.a. av domsbilagan. Samtliga av KeyCard marknadsförda kort och programmerare utgör olovlig avkodningsutrustning. Det sker ständigt förändringar i utbudet av varor som marknadsförs av KeyCard och STOP:s talan avser alla kort och programmerare som marknadsförs på KeyCards webbplats. Talan avser KeyCards svenska verksamhet, nämligen den marknadsföring som riktar sig till svenska konsumenter.

Smarta kort

Det finns, enligt STOP, tre typer av smarta kort, nämligen seriösa smarta kort, eller "applikationskort", ISO 7816-kort och s.k. piratkort.

Seriösa smarta kort, eller applikationskort, är numera frekvent förekommande som bank- och bankomat kort, cashkort, telefonkort, låskort, identitetskort osv. Karaktäristiskt för dessa applikationskort är att de är anpassade för sitt speciella användningsområde samt till helt övervägande del används i tillämpningar där det ställs krav på säkerhet och på begränsning av åtkomsten till den information som finns på kortet eller som kortet skall ge tillgång till. Kortet levereras regelmässigt av tillverkaren eller leverantören av applikationen som kortet skall användas till. Kortet är specialanpassade, både i hård- och mjukvara, för den aktuella tillämpningen och är försedda med specifika spärrar som skall omöjliggöra eller försvåra alternativ användning och annan manipulation.

Seriösa smarta kort tillverkas och levereras av ett begränsat antal producenter, bl.a. Siemens, Philips, Atmel och Motorola. Eftersom de närmast uteslutande används i tillämpningar som fordrar en hög grad av sekretess och säkerhet sker tillverkarnas försäljning och distribution av smarta kort under väl kontrollerade former. I praktiken fordras att en köpare visar en legitim användning för kortet. I stor utsträckning levereras sedan kortet från korttillverkaren specifikt anpassade och programmerade för kundföretagets användningsområde. Med undantag för PCSC-korten förekommer över huvud taget ingen öppen marknad för smarta kort.

Ett undantag från applikationskortet är rena ISO 7816-kort, t.ex. de som följer PCSC-standard (Personal Computer Smart Card) som är en öppen standard för smarta kort att användas med programvara i persondatorer. PCSC har tagits fram av ett antal större dator- och programtillverkare, bl.a. Microsoft, för att tillgodose en förväntad ökad marknad för apparater avsedda för personligt bruk i samband med datorer. PCSC-kortet följer den industriella standarden för smarta kort, ISO 7816, och kan alltså programmeras med en vanlig standardiserad ISO 7816-programmerare, t.ex. Towitoko. Kortet säljs "öppna" och har inget specifikt på förhand angivet användningsområde. De är emellertid inte tomma. Även dessa kort innehåller alltid en grundläggande kommunikationsprogramvara som gör att de kan kommunicera med i första hand standardprogrammerare för ISO 7816-kort.

ISO 7816-standarden är indelad i flera nivåer eller delstandarder, avseende exempelvis kortens fysiska mått, placeringen av kontaktblecken, kontakternas anslutning till elektroniken, olika förfaranden vid programmering respektive läsning osv. Olika typer av kort kan följa standarden ISO 7816 som helhet eller endast följa vissa delstandarder. Det förekommer att smarta kort kallas för ISO 7816-kort redan om de följer vissa grundläggande standardkrav. Smarta kort kallas ofta ISO 7816-kort så snart de till sin yttre form – storlek, tjocklek och kontaktbleckens placering – ser ut som ISO 7816-kort, även om de till sin inre konstruktion inte följer standarden.

Den tredje kategorin av smarta kort är s.k. piratkort. Det är sådana kort som KeyCard säljer. Det är ostridigt att piratkort i grunden är avsedda för TV-avkodning och också används för sådan. Säljare av tomma kort hävdar alltid att korten, vid sidan av TV-avkodning, har en uppsjö av användningsområden, bl.a. till lås och låssystem, att de är vanliga standardkort och att de följer ISO 7816-standarden. Dessa kort säljs helt tomma och innehåller ingen programvara alls. De följer inte ISO-standard och de kan inte programmeras i en standardprogrammerare för ISO-kort. De saknar över huvud taget redovisat användningsområde. Det finns många smarta kort med seriösa tillämpningsområden som inte följer ISO-standard men då har de ett angivet användningsområde. Om ett tomt kort som inte har ett användningsområde skall kunna användas till allehanda realistiska tillämpningar, måste det vara ett standardkort.

Piratkorten är förhållandevis enkla att tillverka. De är uppbyggda av standardkomponenter, en separat mikroprocessor och en separat minneskapsel, som egentligen är avsedda för helt andra ändamål än smarta kort. Kortet saknar därför inbyggd säkerhet och spärrar mot manipulation. Det är också själva poängen med piratkort, eftersom syftet med dem är att de skall kunna manipuleras till att emulera, härma, riktiga applikationskort. Piratkorten avger inte heller någon ATR-signal, vilket krävs enligt ISO 7816-standarden och är nödvändig för att en standardprogrammerare skall kunna identifiera kortet.

De kort som säljs på KeyCards webbplats är piratkort. De är delvis av samma slag (s.k. GULD-kort och varianter på det med PIC-processor från Microchip) som de som prövats av Marknadsdomstolen i de tidigare målen MD 2002:15 och 2002:16. Därutöver förekommer bl.a. även s.k. FUN-kort med ATM-processorer från ATMEL och MII-kort som uppges kunna avkoda Canal Digital. ATM-korten har samma programmeringsarkitektur som de av Marknadsdomstolen tidigare bedömda PIC-korten. Detta innebär att de har den för piratkorten karaktäristiska och från ISO 7816-standarden avvikande "omvända" ledningsdragningen för

programmering, något som följer av att piratkorten inte är bestyckade med särskilda processorer för smarta kort utan med standardprocessorer egentligen avsedda för helt andra ändamål. KeyCards piratkort programmeras inte över kontaktbleck 6 såsom ISO 7816-standarden föreskriver. Korten och programmerarna har en unik uppbyggnad som gör att de endast kan användas tillsammans och i tillämpningar för vilka det finns program skrivna för just dessa programmerare och kort. På ett teoretiskt plan kan piratkort användas till i princip vad som helst. Vad de faktiskt kan användas till beror på vilken programvara som finns tillgänglig att ladda ner från Internet. Den enda programvara som finns allmänt tillgänglig och som kan ge dem ett realistiskt användningsområde är programvara för TV-avkodning. Därmed utgör dessa kort olovlig avkodningsutrustning.

Programmerare för s.k. piratkort

Det förhållandet att piratkorten är bestyckade med processorer som egentligen inte är avsedda för bruk i smarta kort gör att anslutningarna mellan kortets yttre kontaktbleck och processorn inte kan följa ISO 7816-standarden. Korten måste därför programmeras med en programmerare/brännare som är speciellt anpassad för dem. Sådana särskilt anpassade programmerare kan inte användas för att programmera standardkort. Att piratkorten inte heller lämnar någon ATR-signal är ytterligare en avvikelse från standarden som i sig, oberoende av andra avvikelser, medför att ett piratkort inte kan programmeras i en standardprogrammerare för ISO-kort.

Särskilt anpassade programmerare är alltså en nödvändig del för att förse piratkorten med programvara för olovlig avkodning. Teoretiskt kan man med en piratprogrammerare förse piratkort med funktionalitet för allehanda tillämpningar. Detta förutsätter emellertid, liksom beträffande korten, att det finns sådana alternativa tillämpningar för korten och att det finns programvara för den valda tillämpningen att lägga in i korten med programmeraren. Allmänt tillgängligt torde det inte finnas anpassade program att förse piratkorten med, vid sidan av programvara för avkodning av TV-sändningar. Programmerarnas användningsområde är lika begränsat som piratkortens, nämligen att förse korten med programvara för TV-avkodning.

Samtliga programmerare/brännare som KeyCard marknadsför är avsedda för piratkort. Dessa kan endast användas för programmering av piratkort och utgör sådan olovlig avkodningsutrustning vars försäljning strider mot dekoderlagen. Deras enda funktion är att användas med piratkort för att förse dem med avkodningsfunktion. De är konstruerade och särskilt anpassade

för att möjliggöra olovlig tillgång till kodade TV-sändningar. Därmed utgör även dessa programmerare avkodningsutrustning.

Som andrahandsgrund gör STOP gällande att dessa programmerare inte kan användas till annat än att förse piratkort med program för TV-avkodning varför marknadsföring av utrustning med denna enda funktion måste anses strida mot god marknadsföringssed.

Användningsområden för s.k. piratkort och programmerare

Piratkort är i grunden avsedda för TV-avkodning och används för TV-avkodning. Säljare av dessa kort hävdar alltid att korten, vid sidan av TV-avkodning, har en uppsjö av användningsområden, bl.a. till lås och låssystem samt att de är vanliga standardkort och följer ISO 7816-standarderna.

KeyCard hävdar att företaget är inriktat på att sälja låssystem och att man forskar på och utvecklar låssystem samt att de kort och programmerare som företaget säljer är till för att bl.a. användas med dessa lås och låssystem. Enligt STOP:s mening är emellertid inget av de av KeyCard föregivna låsen verkliga eller realistiska användningsområden för piratkort. Under målets gång har KeyCard inventerat marknaden för att finna alternativa användningsområden och har kommit upp med fyra föregivna applikationer där korten ska kunna användas, nämligen SmartIdea, MicroGuard, byggsatsen BR-872 och Free X-TV. Trots KeyCards föregivna inriktning på låssystem förekommer ingen rubrik härom i innehållsförteckningen på KeyCards entrésida på Internet. Först under rubriken "Brännare och kort" finns "Smartcardlås och Säkerhetssystem". Den av KeyCard föregivna inriktningen på lås har inte heller återspeglats i KeyCards sortiment.

Tillverkarna av piratkort framhåller regelmässigt, så även KeyCard, kortens höga minneskapacitet. Det anges t.ex. på KeyCards webbplats om kortet FunCard V 3.0 att det har 8-10 gånger högre och snabbare minne i jämförelse med ett GULD-kort och att det därför har större möjligheter längre fram. När det gäller lås och låsapplikationer behövs mycket litet minne. Att använda kort som innehåller upp till 1000 kb minne är mycket onödigt och överdrivet. På sin höjd behövs några få kb minne. De algoritmer som används vid avkodning av TV-sändningar kräver mycket minne. Hög minneskapacitet möjliggör även att fler kanaler kan avkodas med samma kort.

SmartIdea

Sedan länge har piratkortssäljare hänvisat till SmartIdea som en apparat där piratkorten kan användas. SmartIdea tillverkas av företaget 3 Emme System och är en fullt fungerande anordning för att "låsa" en PC med hjälp av ett smart kort. Utan kort kan apparaten inte startas. Den säkerhet som SmartIdea ger är dock starkt begränsad då hela anordningen lätt kan avlägsnas genom att t.ex. sladden till låset tas bort eller kopplas förbi. Anordningen blir än mer osäker om den dessutom används tillsammans med piratkort, som saknar säkerhet och är lätta att kopiera. Framför allt är SmartIdea onödig. De låsfunktioner SmartIdea erbjuder finns redan inbyggda i alla Windowsprogram och i moderna datorer redan i BIOS (Binary Input/Output System). En låsfunktion i BIOS erbjuder dock en avsevärt mycket högre grad av säkerhet än vad SmartIdea gör. I likhet med andra säkerhetsapplikationer levereras SmartIdea med färdigprogrammerade smarta kort. På tillverkaren 3 Emmes webbsida framgår nämligen att speciella kort, Flashcard med skyddat minne, levereras med SmartIdea. Det finns därför inget behov att köpa piratkort för användning av SmartIdea. Som anförts ovan krävs vidare mycket litet minne, inte mer än 128 byte, för låsapplikationer som SmartIdea, varför det är omotiverat och dyrt att köpa piratkort med stor minneskapacitet. Programmering av piratkort och användning av piratkort till SmartIdea är en tilläggsfunktion som inte fanns med i SmartIdeas första version men som har lagts till nu. I den här tilläggsfunktionen kan man programmera och använda FUN-kort, dvs. en typ av piratkort, men inte PIC-kort. STOP gör således gällande att SmartIdea visserligen fungerar, men den är ganska dyr, har en låg säkerhet – lägre än den som redan finns i datorn – och den är därmed onödig. Den torde ha en försumbar efterfrågan på marknaden. Piratkort är inte nödvändiga för användande av SmartIdea. Enligt STOP:s mening kan SmartIdea inte legalisera piratkorten som ett användningsområde för piratkort.

MicroGuard

Produkten MicroGuard har funnits länge på 3 Emmes webbplats. STOP har försökt beställa låset från 3 Emme som har hänvisat till sina återförsäljare, däribland KeyCard. STOP har också försökt beställa låset från KeyCard. MicroGuard dök emellertid inte upp på KeyCards webbplats förrän i oktober/november 2003. Samtidigt erbjöds ett annat lås benämnt T2000 på webbplatsen. KeyCard kunde dock varken leverera MicroGuard eller T2000. Sedermera har T2000 tagits bort från både 3 Emmes och KeyCards webbsidor och det förelåg leveransproblem beträffande MicroGuard. Först veckan innan huvudförhandlingen löste sig leveransproblemen och ett MicroGuard-lås levererades till STOP. Låset levererades i en kartong som

innehöll en mindre gul öppnad kartong, en svart plastpåse, ett kopplingskort och några sladdar. I den svarta plastpåsen låg SmartIdea, trots att någon sådan inte hade beställts. I den gula kartongen låg MicroGuard. Den gula kartongen var märkt Vimar 16454, 230 V och det fanns ett CE-märke. Vimar är en stor italiensk producent och leverantör av el- och installationsutrustning som tillverkar bl.a. strömbrytare, kontakter, lamparmaturer samt låset Vimar 16454. Låset beskrivs i en av Vimars broschyrer. Där framgår att låset är CE-märkt, avsett för 230 V och att det ska användas antingen med Vimars egna smarta kort eller med ett valfritt ISO-standardkort. Detta stämmer inte med den mycket rudimentära manual som kom med i paketet från KeyCard. Där står att låset ska anslutas till 9 V och inte 230 V. T. S., som på uppdrag av STOP har undersökt låset, fann att elektroniken i låset inte är Vimars, utan att det bara är höljet kring låset som är från Vimar. I övrigt är låset ett hembygge som inte är CE-märkt. Hurvida låset fungerar vet inte STOP. Varken T. S. eller M. F., som på uppdrag av KeyCard och I. F. också har undersökt låset, kunde få det att fungera. Låset från Vimar kostar ca 38 euro. MicroGuard består av hemmagjord elektronik och en SmartIdea och kostar 5 900 kr. Enligt STOP:s mening är den enda förklaringen till detta att skapa ett legitimerat användningsområde för KeyCards piratkort och priset till för att avskräcka kunder så att ingen beställer det.

BR-872

BR-872 är en byggsats som har funnits länge på alla piratkortsäljares webbplatser och uppges vara ett lås. Den tillverkas och säljs ursprungligen av ett företag benämnt Brink. När man bedömer BR-872 skall man vara medveten om att T. B. är en gammal piratkortssäljare som var aktiv redan på 1980-talet och är dömd och förbjuden att sälja piratkort. Han tog då fram en applikation, byggsatsen BR-872, för att det skulle finnas ett annat användningsområde för korten. STOP har under årens lopp förgäves försökt få den att fungera. T. S. har inte lyckats få den att fungera. M. F. påstår i och för sig att han kan få den att fungera, att de tre första byggsatserna han fick från KeyCard var felmonterade och att han vid den sista leveransen lyckades få den att fungera efter byte av komponenter. Det förhållandet att den inte fungerar men har funnits på piratkortssäljares webbsidor under många år visar att det inte finns någon efterfrågan på den. Låset är skådebröd för att visa upp ett föregivet användningsområde för piratkort. Under alla förhållanden är den praktiskt oanvändbar som lås. Den kan kanske användas i undervisningssyfte när det gäller att lära sig löda. Vidare kan den bara användas tillsammans med GULD-kort, som knappast existerar på marknaden längre. Under alla förhållanden legitimeras inga andra kort än GULD-kort med 16F84 processor av byggsatsens existens.

Free X-TV

Free X-TV är ytterligare ett föregivet användningsområde för piratkort och programmerare. Det är en satellitkanal som sänder erotisk film dygnet runt. Något abonnemang fordras inte. Istället finansieras sändningarna delvis genom försäljning av s.k. CAM-moduler som möjliggör tillgång till sändningarna mot en engångsavgift om ca 900 kr. Affärsidén bakom denna abonnemangsform är att sälja moduler för ett högt engångspris och, när marknaden är mättad, lägga ner kanalen eller byta namn och göra en annan ny kanal som fordrar en ny modul. I samband med ett ägarbyte av Free X-TV förra året kodades sändningen om. De moduler som redan hade sålts innan omkodningen blev därmed oanvändbara och behövde uppdateras. Då erbjöd Free X-TV uppdatering på tre olika sätt. Man kunde skicka in sin gamla modul och få den uppdaterad eller beställa och få ett minneskort för ca 8 € med uppdateringsfilen på och med hjälp av kortet uppdatera modulen. Som ett tredje alternativ erbjöds de som hade tillgång till piratkort av typen FUN-kort med minst 32 kB minne samt piratprogrammerare, att från Free X-TV:s webbplats ladda ner en uppdateringsfil som kunde överföras till modulen med hjälp av piratkortet. Behov av uppdatering fanns bara för de moduler som hade köpts före juli 2003. De nya moduler som levereras efter omkodningen och kostar 85-100 € är anpassade till den nya krypteringen och kräver alltså inte någon uppdatering. Uppdateringsmöjligheten med piratkort inspirerade uppenbarligen KeyCard till att skapa ett användningsområde till sina piratkort. Flera månader efter det att det fanns fullt fungerande moduler ute på marknaden började KeyCard sälja gamla, inte uppdaterade moduler, under förevändning att dessa behöver uppdatering med piratkort. KeyCards försäljning av Free X-TV-moduler omfattar tre "paket" bestående av modul respektive modul med kort och programmerare. Paketet med endast en icke uppdaterad modul kostar 995 kr. Övriga paket som består av modul, olika kort och programmerare, är betydligt dyrare och kostar 1 900 – 2000 kr. Det behövs inte piratkort för att uppdatera de moduler som KeyCard säljer utan det går att använda ett enkelt minneskort för det.

De Free X-TV-moduler som KeyCard marknadsför på den engelskspråkiga versionen av webbplatsen fordrar inte någon uppdatering. Det är således endast vid beställning från Skandinavien som moduler som fordrar uppdatering erbjuds. Att KeyCard, flera månader efter det att det fanns fullt fungerande moduler på marknaden för ca 900 kr att köpa, i Skandinavien började sälja gamla moduler som måste uppdateras är enligt STOP resultatet av en medveten och aktiv manipulation från KeyCards sida med syfte att på den skandinaviska marknaden ge

intryck av att det finns ett legitimt användningsområde för piratkort och programmerare till dessa.

Såvitt avser den produkt som KeyCard hänvisar till som är under utveckling framgår av de åberopade handlingarna att det handlar om att utveckla ett låssystem för en ATMEL-processor som heter AVR3232 som är en säker mikrodata och inte en sådan som finns i FUN-korten.

Sammanfattningsvis menar STOP att de omstridda korten och programmerarna till dessa är avsedda att användas för TV-avkodning. De alternativa applikationerna som KeyCard hänvisar till är konstruerade och utan praktiska motiv. De kan inte legitimera förekomsten av piratkort.

Medverkansansvar

I. F. finns upptagen bland ledande personer på KeyCards webbplats. Han är den person som förestår och praktiskt sköter den svenska verksamheten i Vejbystrand. Han är också mantalskriven och bor på den adress som uppges vara KeyCards svenska adress och där KeyCards svenska verksamhet bedrivs.

Även om han inte kan anses vara näringsidkare i och för sig, är han i vart fall sådan medverkande som avses i 14 § 2 st MFL.

KeyCard och I. F.

STOP:s talan skall ogillas eftersom KeyCard inte bedriver någon marknadsföring i Sverige. Försäljningen i Vejbystrand kan inte anses som marknadsföring i MFL:s mening. I vart fall skall STOP:s talan ogillas då det inte föreligger förutsättningar för Marknadsdomstolen att begränsa den fria rörligheten för de informationssamhällets tjänster som KeyCard tillhandahåller. Under alla förhållanden utgör de i målet aktuella produkterna inte olovlig avkodningsutrustning, eftersom det finns ett antal reella och seriösa alternativa användningsområden för dessa produkter. Vidare bestrids att marknadsföring av de aktuella programmerarna strider mot god marknadsföringssed.

I. F. gör för egen del gällande att han inte har medverkat till eller bedrivit någon marknadsföring.

Enligt KeyCards mening kan ett "piratkort" knappast existera förrän ett tomt kort har programmerats så att innehavaren kan ta del av innehållet i kodade TV-sändningar. Eftersom de kort KeyCard saluför är oprogrammerade och syftar till annan användning än avkodning av kodade TV-sändningar är termen smarta kort mer rättvisande.

Vad STOP betecknar som den för piratkorten karaktäristiska, och från ISO 7816-standarden avvikande "omvända" ledningsdragningen för programmering, saknar helt betydelse för om de kort som KeyCard säljer kan anses utgöra avkodningsutrustning.

MFL:s tillämplighet

Den verksamhet som KeyCard bedriver i Sverige utgörs endast av försäljningsverksamhet, dvs. beställningar tas emot och verkställs. Uppgifterna på KeyCards webbsida kan inte ändras eller påverkas från Sverige. Webbsidan är dansk och ligger på en dansk server och under den finns den svenskspråkiga och den engelskspråkiga versionen. Samtliga beslut rörande hemsidan fattas i Danmark. Eftersom STOP:s talan omfattar KeyCards verksamhet i och från Sverige och då KeyCard inte vidtar några marknadsföringsåtgärder i eller från Sverige är MFL inte tillämplig. I konsekvens härmed skall STOP:s talan ogillas.

E-handelslagen

Det saknas förutsättningar för Marknadsdomstolen att enligt lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster (e-handelslagen) begränsa den fria rörligheten för de informationssamhällets tjänster som KeyCard tillhandahåller. Begreppet informationssamhällets tjänster innefattar bl.a. försäljning av varor. KeyCard utgör en tjänsteleverantör i e-handelslagens mening. Då KeyCards etableringsstat är annan än Sverige får domstol endast begränsa den fria rörligheten för en sådan informationssamhällets tjänst för att skydda allmän ordning eller säkerhet, folkhälsan eller konsumenter. Sådana förutsättningar föreligger inte.

Närmare om KeyCard och dess verksamhet

KeyCard har en relativt stor verksamhet, framför allt i Danmark, med ett tiotal anställda och två försäljningsställen. KeyCards affärsidé var inledningsvis att sälja dörrlås-system i form av byggsatser samt säkerhetssystem till datorer till förhållandevis låga priser. De säkerhetssystem som fanns på marknaden år 1998 då företaget grundades var ofta för dyra för att en privatperson skulle ha råd att införskaffa dem. Det fanns därför en marknad för säkerhetssystem där tekniken med smarta kort och brännare utnyttjades. Sedan starten har KeyCard successivt utökat sitt sortiment och saluför idag allt inom Playstation, tillbehör till datorer, parabolantennor och mobiltelefoni. Sortimentet består av drygt tusen olika artiklar. KeyCard bedriver också ett omfattande utvecklingsarbete i syfte att ta fram nya, förbättrade inpasserings- och säkerhetssystem m.m. En stor del av försäljningen utgörs också av kort och programmerare. Sedan en tid pågår dessutom utredning om möjligheten att patentera hela eller delar av säkerhetssystem som KeyCard har utvecklat.

KeyCard anser sig vara oförhindrad att sälja och marknadsföra de i målet aktuella produkterna i Danmark. STOP har stämt KeyCard i Sverige av den enkla anledningen att förutsättningarna för att få bifall till sin talan är större här än i Danmark.

KeyCard har som policy att vägra försäljning om det finns indikationer på att syftet med att köpa korten är piratavkodning. Om en kund frågar KeyCard hur man ska bära sig åt för att avkoda en TV-sändning meddelar KeyCard att det inte är tillåtet och uppmanar kunden att skicka tillbaka produkterna till KeyCard. KeyCard har vidare som policy att medverka till brottsutredningar.

KeyCards kunder utgörs av både privatpersoner och företag. Företagen är ofta små eller medelstora. KeyCard har varit i kontakt med en del av dessa företag för att få reda på hur korten används. Tyvärr har flera av företagen inte velat medverka när de har hört att STOP är inblandat. De har sagt att de inte vill bli inblandade och att KeyCard inte får hänvisa till dem. Bland KeyCards kunder finns emellertid bl.a. svenska Försvarmakten, som är en mycket stor kund, liksom Sony Ericsson. Därutöver finns lasarett, larmföretag, skolor, sjukhem och åkerier. Några av de företag som inte velat medverka har dock förklarat att korten används till t.ex. inpasserings- och säkerhetssystem, utbildning, access till datorer, tändningsnycklar och utveckling av egna applikationer. Ett larmföretag förklarade att de använder korten när de byter larm.

I. F.

I. F. är endast anställd av KeyCard och saknar egna ägar- eller vinstintressen. Han har inte själv bedrivit någon marknadsföring och har inte väsentligen bidragit till någon sådan. Den verksamhet som bedrivs i Vejbystrand består endast i att ta emot och verkställa beställningar som kommer in. I. F. har inte haft någonting med utformningen eller innehållet på KeyCards hemsida att göra. Han saknar möjligheter att lägga till, ändra eller ta bort uppgifter på KeyCards hemsida eftersom dataservern för KeyCards hemsida finns i Danmark. I. F. har inte förvarat ett stort antal varor och handlingar rörande KeyCards svenska verksamhet i sin bostad. Den husrannsakan som företogs ägde endast rum i KeyCards lokaler och inte i I. F:s bostad.

Användningsområden för i målet aktuella produkter

Det finns ett antal reella och seriösa alternativa användningsområden för tomma smarta kort och programmerare. Vidare sker kontinuerligt en utveckling på området och användningen av smarta kort och programmerare ökar. Biltillverkaren Honda ska t.ex. lansera ett startsystem för bilar där ett smartcard används i stället för startnyckel.

SmartIdea är ett datasäkerhetssystem för Windowsbaserade datorer. Det finns möjligheter att utveckla nya produkter där SmartIdea ingår. SmartIdea är väl lämpad för miljöer där det finns flera användare till varje dator och där det även erfordras att behörighetsgraden varierar mellan användarna. SmartIdea skall integreras i datorn. Det är riktigt att korten kan kopieras. KeyCard saluför ett stort antal produkter utöver de i målet aktuella. Detta är troligen förklaringen till varför kunder väljer att köpa SmartIdea och smarta kort avsedda härför från KeyCard i stället för från tillverkaren. Många kunder vill göra alla sina inköp från samma leverantör och dessutom torde KeyCards priser stå sig väl från konkurrenssynpunkt. KeyCard erbjuder sina kunder tryck på de kort som säljs vilket givetvis är av intresse för t.ex. skolor, då korten som levereras kan förses med skolans och kortinnehavarens namn m.m. Efterfrågan på SmartIdea är inte liten. Det standardkort som SmartIdea levereras med är som en huvudnyckel som skall stoppas in i bankfacket.

PIC-korten kan bl.a. ingå som delar i färdigutvecklade system som finns på marknaden idag för tidsregistrering ("stämpelklocka"). Det finns hårdvara som möjliggör utveckling av system

där PIC-kort fungerar som passerkort. PIC-korten kommer snart att fungera tillsammans med SmartIdea.

FUN-kort kan användas med SmartIdea och har dessutom, genom den frihet de medger för kommunikationssätt med kortläsaren, stor potential för användning i nya typer av lösningar för smarta kort.

Mastera IV och StarLight Advance/CardMaestro kan tillsammans med på Internet fritt tillgänglig mjukvara och SimCard Adaptor användas för att redigera adresslistan på SIM-kort avsedda för mobiltelefoner.

Övriga programmerare kan användas för att initiera FUN-kort så att de följer ISO 7816-3 vilket t.ex. krävs för att de ska fungera tillsammans med SmartIdea.

KeyCard är sedan en tid exklusiv återförsäljare av Free X-TV-moduler. Free X-TV är ett system som tillhandahålls av Canal Europe Audivisuel i Luxemburg och som visar erotisk film dygnet runt. En köpare av en sådan modul får ett livstids abonnemang. De moduler som KeyCard tillhandahåller uppdateras av abonnenterna själva med användning av smarta kort, FUN-kort version 5.0 eller 7.0 och programmerare. På KeyCards hemsida finns därför kombinationserbudanden där Free X-TV-moduler säljs tillsammans med smarta kort och programmerare till låga priser. Även om det på marknaden nu existerar moduler där uppdatering inte erfordras utgör ändå uppdatering av moduler ett användningsområde för de i målet aktuella produkterna. Dessutom är köparen vid inköp av programmerare och kort inte hänvisad enbart till att uppdatera sin modul vid det första användningstillfället. Även framtida uppdateringar kan utföras.

BR-872 är ett dörrlås-system och en viktig produkt för KeyCard. Genom KeyCards försorg har flera prototyper tagits fram där det aktuella låset har monterats på en dörr. Dessa prototyper kommer inom kort att presenteras på KeyCards webbsida. KeyCard har också kontaktats av ett företag som säljer dörrlås m.m. som framdeles kommer att sälja låsen och även ha utställningsexemplar framme i sin butik. BR-872 är även lämpligt för utbildningsändamål.

Inom KeyCards utbud av lås- och säkerhetssystem där den aktuella tekniken utnyttjas finns även MicroGuard. Det är ett låssystem som främst syftar till att användas på t.ex. hotell där

man har många användare. Fördelen med att utnyttja smarta kort i sådana sammanhang är att de har en längre livslängd än vad magnetkort har.

KeyCards mest prioriterade projekt just nu är ett låssystem som är under utveckling. KeyCard har fört långtgående förhandlingar med en tillverkare av detta prismässigt konkurrenskraftiga dörrlåssystem. Systemet är tänkt att kunna användas både inomhus och utomhus och är lämpat för t.ex. inpassering inom småindustri, kontor och privata fastigheter samt för interna inpasseringssystem inom företag. KeyCard har hittills betalat miljonbelopp till ett programmeringsföretag för att utveckla programvara för just detta låssystem.

STOP har genmält följande.

KeyCard, vars svenska version av webbplatsen uppenbart riktar sig till Sverige och till svenska konsumenter, bedriver marknadsföring i Sverige. Begreppet marknadsföring omfattar bl.a. försäljning. KeyCard och I. F. bedriver verksamhet i form av e-handel i och från Sverige och denna verksamhet innefattas i begreppet marknadsföring. MFL är därtill tillämplig på marknadsföring från utlandet som väsentligen riktar sig till svenska konsumenter. KeyCard bedriver ostridigt verksamhet i Sverige. Därmed är MFL och dekodeklagen tillämpliga, oavsett om moderbolaget finns i Danmark och oavsett om beställningarna går via en server i Danmark. Även webbplatsen är marknadsföring i Sverige, oavsett om den administreras från Danmark.

STOP ifrågasätter inte att I. F. endast är anställd av KeyCard. Då han är den som sköter verksamheten i Sverige är han ändå att anse som medverkande enligt MFL. Det saknar betydelse att han eventuellt inte har några ägar- eller vinstintressen i KeyCard. Han är djupt involverad i och chef för verksamheten i Sverige. Verksamheten bedrivs från hans fastighet och hela hans familj är engagerad i den. Han fakturerar och sköter de svenska räkenskaperna, sköter all kundhantering och fattar dagligen beslut om den svenska verksamheten som ligger på en sådan nivå att hans medverkan måste omfattas av MFL.

STOP bestrider att e-handelslagen på något sätt hindrar ett bifall till STOP:s talan. E-handelslagen är över huvud taget inte tillämplig. Den gäller inte regler med avseende på vilka varor som får eller inte får marknadsföras. Även om Marknadsdomstolen skulle finna att e-handelslagen är tillämplig följer det av lagens lagvalsregler att det är lagen i det land där den marknadsförda verksamheten bedrivs som gäller. I förevarande fall är det Sverige. I e-handelslagen

finns det dessutom undantag för att tillgodose bl.a. allmän ordning. Att ingripa mot marknadsföring av avkodningsutrustning, som är förbjuden enligt såväl nationell rätt som EG-rätt, är alltid proportionerligt i enlighet med undantaget. Såväl den svenska MFL som dekodeklagen är tillämpliga på KeyCards verksamhet i Sverige.

Det är inte korrekt att STOP har valt att stämma KeyCard i Sverige därför att de aktuella produkterna är tillåtna i Danmark. Enligt STOP Danmark är KeyCard stämda i Danmark och där pågår för närvarande ett mål mot KeyCard där STOP har valt att yrka på skadestånd i stället för förbud. Danmark har samma inställning till avkodningsutrustning som den som gäller i Sverige.

STOP motsätter sig att ett förbud inskränks till att avse försäljning till köpare som inte intygar att utrustningen skall användas till annat än otillåten avkodningsutrustning. Ett sådant förbud skulle sakna lagligt stöd. Därtill kommer att sådana intyganden är omöjliga att kontrollera samt att användning av piratkort för TV-avkodning inte är otillåten hos konsumenten/intyggivaren varför sanningsenligheten i intyget inte har rättslig relevans för denne. I den mån en köpare önskar kort för annan användning än TV-avkodning finns det andra och billigare kort att tillgå på marknaden.

BEVISNING

Parterna har åberopat omfattande skriftlig bevisning.

STOP har som muntlig bevisning åberopat vittnesförhör med säkerhetskonsulten T. S.

KeyCard och I. F. har som muntlig bevisning åberopat förhör under sanningsförsäkran med R. P. och I. F. Vidare har KeyCard och I. F. åberopat vittnesförhör med K. G., filosofie licentiat och forskarstuderande vid Chalmers Tekniska Högskola, M. F., civilingenjör i datateknik från Chalmers Tekniska Högskola, samt med H. S.

R. P. och I. F. har i allt väsentligt bekräftat de uppgifter KeyCard och I. F. lämnat sakframtällningsvis.

T. S., K. G. och M. F. har hörts mot varandra och berättat om vad de funnit vid sina respektive undersökningar av den i målet aktuella utrustningen.

H. S. har berättat om att det företag han är anställd vid köper kort från KeyCard för att användas i stället för nycklar i låssystem.

DOMSKÅL

STOP har i första hand yrkat förbud för KeyCard och I. F. att i Sverige marknadsföra sådan avkodningsutrustning som inte får yrkesmässigt marknadsföras eller överlåtas här i landet. Enligt STOP utgör samtliga de tomma kort och programmerare som KeyCard tillhandahåller avkodningsutrustning i dekodeklagens mening.

KeyCard och I. F. har invänt att KeyCard inte bedriver någon marknadsföring i Sverige, att det skulle strida mot den EG-rättsliga principen om fri rörlighet för varor och tjänster att förbjuda marknadsföring av de aktuella produkterna samt att de tomma korten och programmerarna under alla förhållanden har flera legala användningsområden, varför de inte kan anses utgöra avkodningsutrustning i dekodeklagens mening. Vidare har I. F. för egen del invänt att han inte har medverkat till KeyCards marknadsföring varför STOP:s talan mot honom i första hand skall avvisas och i andra hand ogillas.

Under målets handläggning har STOP som andrahandsgrund för förbudsyrkandet avseende programmerarna åberopat att dessa inte kan användas till något annat än att förse s.k. piratkort med program för TV-avkodning och att marknadsföring av utrustning med denna enda funktion måste anses strida mot god marknadsföringssed. KeyCard och I. F. har häremot i första hand gjort gällande att STOP därmed har gjort en otillåten taleändring. I andra hand har KeyCard och I. F. bestritt att marknadsföring av programmerarna strider mot god marknadsföringssed. Enligt Marknadsdomstolens mening utgör STOP:s andrahandsgrund inte någon ändring av saken och därmed föreligger inte något formellt hinder mot att pröva STOP:s talan i denna del. Marknadsdomstolen lämnar därför detta avvisningsyrkande utan bifall.

MFL:s tillämplighet

Enligt 2 § MFL är lagen tillämplig då näringsidkare marknadsför eller själva efterfrågar produkter i sin näringsverksamhet. Någon begränsning av lagens tillämplighet beträffande medier som kan komma till användning vid marknadsföring har inte gjorts. MFL är sålunda även tillämplig på marknadsföring som förekommer på Internet (se bl.a. MD 2000:8, MD 2000:19 och MD 2001:19). Avgörande för om MFL bör tillämpas på en marknadsföringsåtgärd är i

stället om åtgärden är inriktad på en svensk publik, dvs. konsumenter och näringsidkare i Sverige. Det saknar betydelse varifrån en marknadsföringsåtgärd företas. MFL kan således tillämpas på marknadsföringsåtgärder som distribueras till svensk publik från utlandet (se MD 1989:6). Den påtalade marknadsföringen på KeyCards webbsida finns i en svensk version med prisuppgifter angivna i svenska kronor. Vidare är en svensk adress i Vejbystrand uppgiven, liksom svenska telefonnummer för beställning och support m.m. Redan på grund härav är det uppenbart att den påtalade marknadsföringen på Internet är riktad mot konsumenter på den svenska marknaden. Det förhållandet att den påtalade marknadsföringen förekommer på en webbsida med en dansk webbadress utgör i sig således inte något skäl att, som KeyCard och I. F. har yrkat, ogilla STOP:s talan.

De aktuella produkterna

Enligt STOP utgör samtliga tomma kort och programmerare som KeyCard marknadsför på sin webbplats avkodningsutrustning i deko­derlagens mening och marknadsföring av korten och programmerarna är därför olaglig och bör förbjudas. KeyCard å sin sida har bestritt att de tomma korten och programmerarna utgör avkodningsutrustning eftersom den tekniska utvecklingen numera har gått så långt att det finns legala användningsområden för produkter av ifrågavarande slag.

Enligt 4 § deko­derlagen avses med avkodningsutrustning sådan utrustning eller programvara som har utformats eller anpassats för att göra en tjänst som omfattas av lagen tillgänglig i tolkningsbar form. TV-sändning är sådan tjänst. Enligt 5 § samma lag får avkodningsutrustning inte yrkesmässigt eller annars i förvärvssyfte tillverkas, importeras, distribueras, säljas, hyras ut, innehas, installeras, underhållas eller bytas ut i syfte att göra en tjänst som omfattas av lagen tillgänglig i tolkningsbar form utan tjänsteleverantörens godkännande. Lagen, som föranletts av Europaparlamentets och rådets direktiv 98/84/EG, ersatte en tidigare lag med samma namn (SFS 1993:1367).

Marknadsdomstolen har i avgörandena MD 2002:15 och 2002:16 funnit s.k. tomma kort utgöra olovlig avkodningsutrustning. Till grund för denna slutsats låg utlåtanden från Statens kriminaltekniska laboratorium (SKL) och uppgifter från M. F., som då arbetade vid SKL och som utförde de aktuella undersökningarna. Marknadsdomstolen fann i dessa avgöranden – mot bakgrund av uppgifterna i utlåtandena och nämnda vittnesmål och i avsaknad av utredning som talade i annan riktning – att de undersökta korten var konstruerade för att avkoda

TV-sändningar och att de rimligen inte hade något annat praktiskt användningsområde, till följd varav korten omfattades av förbudet i dekodeklagen. I avgörandet MD 2003:30 fann inte Marknadsdomstolen anledning att göra någon annan bedömning än den domstolen tidigare hade gjort.

I förarbetena till den tidigare gällande dekodeklagen (prop. 1993/94:53 s. 24 f.) angavs bl.a. följande. Avkodningsutrustning kan vara av många slag. Om den är konstruerad för att, ensam eller tillsammans med annan anordning, bereda tillgång till en eller flera kodade sändningar eller särskilt anpassad för detta ändamål, är den en avkodningsutrustning. S.k. smart-cards är också att betrakta som avkodningsutrustning, liksom den del av utrustningen ett sådant kort skall kopplas ihop med. Med smart-card avses ett datakort som besitter kunskapen om hur avkodning skall ske. Lagrådet har dock påpekat att för att en del till en avkodningsutrustning eller en byggsats till en avkodningsutrustning i sig själv skall kunna betraktas som en avkodningsutrustning torde få krävas inte endast att delen är nödvändig för avkodningsfunktionen utan också att den inte kan ha någon annan funktion. Att avkodningsutrustning har andra funktioner, av vilken avkodningsförmågan bara är en, hindrar inte att utrustningen omfattas av denna lag. Utrustningen kan ha förmåga att avkoda en eller flera sändningar och kan utgöras av en byggsats eller en del av en sådan.

I den nu gällande dekodeklagens förarbeten (prop. 1999/2000:49 s. 14 f.) framhålls att utformningen av direktivet 98/84/EG inte har inriktats på vissa tydligt avgränsade former av utrustning eller att peka ut vissa tekniska lösningar. En sådan teknik baserad på en eller flera konkreta tillämpningar har undvikits för att minska riskerna för att t.ex. modifieringar av programvara leder till att bestämmelsen lätt kan kringgå. En så teknikberoende reglering som möjligt har således eftersträvat och av dessa skäl föreslås inte någon närmare definition av vilken utrustning det kan bli fråga om. Det otillåtna ligger i det sätt på vilket avkodningsutrustningen är avsedd att användas, nämligen att möjliggöra otillåten tillgång till en skyddad tjänst. Det är således inte avkodningsutrustningen i sig som är otillåten utan olika slag av kommersiell verksamhet med sådan utrustning.

Marknadsdomstolen gör följande bedömning.

I förevarande mål är ostridigt att de tomma kort och programmerare som säljs på KeyCards webbplats kan användas för TV-avkodning. Den som vill låta avkoda en kodad TV-sändning utan tjänsteleverantörens tillstånd är således hänvisad antingen till färdigprogrammerade kort,

vilka numera torde vara förhållandevis sällsynta, eller till den typ av kort och programmerare som bl.a. KeyCard säljer. Det är också ostridigt i målet att tomma kort och programmerare av ifrågavarande slag ursprungligen har konstruerats för att användas till olovlig TV-avkodning. Genom utredningen i målet, bl.a. vad T. S. har uppgett, står det också klart att de tomma kortens utveckling hela tiden har följt utvecklingen av TV-bolagens försök att hindra otillåten avkodning.

De alternativa användningsområden som KeyCard har angett är bl.a. SmartIdea, MicroGuard, BR-872, Free X-TV, forskning, utveckling och utbildning. KeyCard har också nämnt ett nytt låssystem som är under utveckling och som KeyCard förväntar sig ska bli en storsäljare. KeyCard har bl.a. åberopat utskriften från olika webbplatser med viss information om de angivna produkterna. M. F. och K. G. har uppgett att flera av de av KeyCard angivna produkterna kan användas på beskrivet sätt. De har också beskrivit den utvecklingspotential som finns i de aktuella produkterna.

Även om SmartIdea, BR-872, uppdatering av Free X-TV-moduler och eventuellt också MicroGuard kan fås att fungera enligt beskrivningarna, är det enligt Marknadsdomstolens bedömning emellertid osannolikt att de aktuella produkterna inhandlas från KeyCard för dessa uppgivna ändamål. Det finns inte heller någon utredning som visar i vilken omfattning dessa applikationer faktiskt inhandlas. KeyCards påstående om att dess kunder, som använder i målet aktuella produkter till annat än TV-avkodning, är så rädda för STOP att de inte vill medverka i rättegången ter sig märkligt med hänsyn till att sådan användning inte är olaglig. Påståendet om en framtida utvecklingspotential för de aktuella produkterna kan inte anses innebära att de för närvarande har ett reellt praktiskt användningsområde. Sammanfattningsvis anser Marknadsdomstolen att det av utredningen inte framgår att de tomma kort och programmerare som KeyCard marknadsför på sin webbsida rimligen kan ha andra praktiska användningsområden än just TV-avkodning. Enligt Marknadsdomstolens mening omfattas därmed samtliga av KeyCard marknadsförda tomma kort och programmerare av förbudet i deko-derlagen.

Marknadsföring som sker på ett sätt som står i strid med tvingande lagstiftning är att anse som otillbörlig i MFL:s mening.

Såvitt gäller särskilt KeyCards och I. F:s invändning om att ett bifall till STOP:s talan skulle strida mot EG-rätten, gör Marknadsdomstolen följande bedömning.

Syftet med direktivet 98/84/EG, som föranlett dekoderlagen, är enligt artikel 1 att tillnärma bestämmelserna i medlemsstaterna om åtgärder mot olaglig utrustning som ger obehörig tillgång till skyddade tjänster. Av punkterna 11 och 12 i direktivets preambel framgår också att skillnader i nationella regler om rättsligt skydd för tjänster som bygger på eller utgörs av villkorad tillgång kan skapa hinder för den fria rörligheten för varor och tjänster och att det inte räcker med att tillämpa fördraget för att undanröja dessa hinder för den inre marknaden. Direktivet ställer krav på medlemsländerna att förbjuda och tillgripa lämpliga sanktioner mot ett brett spektrum av kommersiella verksamheter som gäller illegala avkodare. Mot bakgrund härav är det uppenbart att principen om fri rörlighet för varor och tjänster inte syftar till att skydda tillhandahållandet av olovlig avkodningsutrustning. Något hinder mot att bifalla STOP:s talan föreligger därför inte på denna grund.

Vid denna bedömning skall KeyCard förbjudas att marknadsföra sådana kort och programvaror som domstolen nu funnit utgöra avkodningsutrustning.

Förbudet bör emellertid få en något annorlunda utformning än vad STOP har yrkat.

Medverkansansvar

Bestämmelsen i 14 § första stycket MFL enligt vilken en näringsidkare, vars marknadsföring strider mot god marknadsföringssed eller på något annat sätt är otillbörlig mot konsumenter eller näringsidkare, får förbjudas att fortsätta med den marknadsföringen eller att vidta någon annan liknande åtgärd kompletteras i paragrafens andra stycke med en bestämmelse enligt vilken ett förbud också får meddelas en anställd hos näringsidkaren, någon annan som handlar på näringsidkarens vägnar och var och en som i övrigt väsentligt har bidragit till marknadsföringen.

STOP har – utan att åberopa någon närmare utredning härom - gjort gällande att I. F. är sådan medverkande som avses i 14 § andra stycket MFL. I. F. har bestritt att så är fallet och förklarat att han inte på något sätt har medverkat vid marknadsföringen.

Marknadsdomstolen gör följande bedömning.

Väl framgår av utredningen i målet att I. F. är anställd av KeyCard, att hans bostad är på samma adress som den adress KeyCard uppger sig ha i Sverige och att hans arbetsuppgifter består av att ta emot och verkställa beställningar av KeyCards produkter till svenska kunder. Det är emellertid inte visat att han haft sådan ställning i KeyCard eller kunnat utöva sådant inflytande över KeyCards verksamhet eller att han i övrigt faktiskt har bidragit till marknadsföringen på ett sådant sätt som erfordras för medverkansansvar enligt MFL. STOP:s talan mot I. F. skall därför ogillas.

Vite

Ett förbud skall enligt 19 § MFL förenas med vite om det inte av särskilda skäl är obehövligt. Sådana särskilda skäl föreligger inte.

Rättegångskostnader

Vid denna utgång skall KeyCard förpliktas att ersätta STOP viss del av dess rättegångskostnader och STOP skall förpliktas att ersätta I. F. dennes rättegångskostnader.

STOP har yrkat ersättning för sina rättegångskostnader med 767 915 kr, varav 607 200 kr avser ombudsarvode. STOP har vidare förklarat att den del av kostnaderna som uteslutande avsett talan mot I. F. uppgår till 10 000 kr. STOP har därutöver anfört att rättegångskostnaderna i målet inte kan hänföras till den ene eller den andre motparten då kostnaderna skulle ha uppgått till samma belopp om talan hade väckts enbart mot den ena motparten. Utredning och annat arbete i målet har avsett den påtalade utrustningens legala status och har varit oberoende av antalet svarandeparter.

KeyCard och I. F. har gemensamt yrkat ersättning för sina rättegångskostnader med 1 066 926 kr, varav 716 000 kr avser ombudsarvode, 247 036 kr avser kostnader för sakkunnigbevisning, 87 279 kr avser förbrukat material och 16 611 kr avser övriga utlägg. KeyCard och I. F. har förklarat att deras rättegångskostnader inte kan hänföras till den ena eller den andra parten och att om en uppdelning måste ske, kostnaden får delas lika mellan KeyCard och I. F.

Parterna har, med undantag för KeyCards och I. F:s yrkande avseende förbrukat material där STOP vitsordat ett belopp om 25 000 kr, vitsordat de av motparterna yrkade beloppen som skäligen i och för sig.

STOP:s yrkande i sak riktar sig mot både KeyCard och I. F. och yrkandet bygger på huvudsakligen samma grunder. STOP har vunnit bifall till sin talan mot KeyCard men förlorat sin talan mot I. F. Enligt STOP kan bolagets rättegångskostnader inte med något särskilt belopp hänföras till den ene eller den andre svaranden, bortsett från 10 000 kr som enbart avser bolagets talan mot I. F. Vid sådant förhållande bör KeyCard förpliktas utge hälften av det av STOP yrkade beloppet efter avdrag av de 10 000 kr som uteslutande är att hänföra till I. F. Om beloppen i denna del råder inte tvist.

STOP, å sin sida, skall ersätta I. F:s rättegångskostnader, vilka – med stöd av föreliggande uppgifter – måste anses utgöra hälften av svarandeparternas gemensamma kostnader. När det gäller yrkandet avseende ersättning för förbrukat material finner Marknadsdomstolen att ett belopp om 40 000 kr är skäligt i och för sig. Om beloppen i övrigt råder inte heller i denna del tvist.

På Marknadsdomstolens vägnar

C H Fallenius

Ledamöter: Christer Fallenius, ordförande, Ingegerd Westlander, Ingrid Larén Marklund, Kerstin af Jochnick, Lars-Gunnar Mattsson och Anders Stenlund. Enhälligt

Sekreterare: Malin Nyman