



DET KONGELEGE  
JUSTIS- OG POLITIDEPARTEMENT

# Ot.prp. nr. 51

(2000-2001)

---

Om lov om endring av straffeloven § 262  
(rettsleg vern av koda tenester)

*Tilråding frå Justis- og politidepartementet av 30. mars 2001,  
godkjend i statsråd same dagen.*

## 1 Hovudinnhaldet i proposisjonen

Justisdepartementet gjer i proposisjonen framlegg om å endre straffeloven (strl.) § 262. Noverande føresegn gjer det straffbart å skaffe seg eller andre rettsstridig tilgang til koda radio- og fjernsynsignal. I dei seinare åra har det kome til ei rekkje nye koda elektroniske tenester, som mellom anna videogram og fonogram på bestilling, som ikkje er dekkja av omgrepet «fjernsyns- eller radiosignal» i strl. § 262. Desse tenestene - gjerne omtala som «informasjonssamfunnstenester», jf. definisjonen i kapittel 3.2 - har difor ikkje same vern mot spreiking og bruk av «piratdekodere» mm. som dei eldre tenestene.

Siktemålet med endringsframlegget er å gi eit rettsleg vern til alle såkalla «informasjonssamfunnstenester». Ei slik lovendring vil også sikre gjennomføring i norsk rett av direktiv 98/84/EF av 20. november 1998 om rettsleg vern av tilgangskontrollerte og tilgangskontrollerande tenester. Direktivet vart ein del av EØS-avtalen ved EØS-komiteen si avgjerd 23. februar 2001, avgjerd nr. 17/2001. Utanriksdepartementet fremmer samtidig med denne odelstingsproposisjonen ein stortingsproposisjon om samtykke til godkjenning av vedtaket i EØS-komiteen. Lovframlegget er dessutan i samsvar med Europarådskonvensjonen om rettsleg vern av tilgangskontrollerte og tilgangskontrollerande tenester («European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access»), vedteke av Ministerkomiteen i Europarådet 6. oktober 2000. Regjeringa vedtok ved kongeleg resolusjon 19. januar 2001 å underteikne konvensjonen.

Utover det EØS-rettslege vil endringsframlegget gi ei betre redigert føresegn, m.a. med differensiert strafferamme etter alvoret i lovbrottet.

## 2 Høyring

Justisdepartementet sendte 1. mars 2000 ut eit høyringsbrev om endring av straffeloven § 262. Om bakgrunnen for endringsframlegget vart det mellom anna sagt:

«I dette høringsnotatet blir det foreslått endring av straffeloven (strl.) § 262. Primærmålet med endringsforslaget er å sikre en fullstendig gjennomføring av Europaparlaments- og rådsdirektiv 98/84/EF av 20. november 1998 om rettslig vern av tilgangskontrollerte og tilgangskontrollerende tjenester i norsk rett.

Departementet benytter samtidig anledningen til å foreslå en omfattende omredigering av bestemmelsen. Vi ønsker å gjøre den lettere tilgjengelig samtidig som skillet mellom forbudet mot kommersiell spredning av dekodingsutstyr og forbudet mot privat bruk av slikt utstyr kommer klarere fram.

I tillegg foreslås kriminalisering av visse befatningsmåter med dekodingsutstyr som verken er omfattet av gjeldende strl. § 262 eller av EU-direktivet. ..(..).

Gjeldende straffelov § 262 beskytter krypterte og kodete fjernsyns- og radiosignaler. Direktivet krever i tillegg at såkalte «informasjons-samfunnstjenester» skal beskyttes i det enkelte medlemsland, når disse er kryptert/kodet av hensyn til vederlagsinteressen. Slike tjenester vil per i dag typisk være videogrammer og fonogrammer på forespørsel samt internett-tjenester man ikke får tilgang til uten betaling av vederlag. Den teknologiske utviklingen vil ventelig gi et stadig økende utbud av slike tjenester.

I dag taper de bransjene som tilbyr slike tjenester i kryptert form, inntekter ved at det omsettes utstyr, programvare eller koder som gjør det mulig å få tilgang til disse tjenestene i forståelig form uten å betale vederlag til rettighetshaverne. Ofte vil muligheten for å ta betaling være en grunnforutsetning for at slike tjenester blir tilbudt markedet. Manglende effektiv rettslig beskyttelse av vederlagsinteressen kan derfor føre til et mindre tilbud av slike tjenester enn det som er kulturpolitisk ønskelig.

Forløperen til direktiv 98/84/EF er Kommisjonens grønnbok om «Rettslig beskyttelse av kodete tjenester i det indre marked». ..(..).

Høyringsbrevet gjekk til følgjande instansar:

Departementa

Høgsterett

Lagmannsrettane

Riksadvokaten

Statsadvokatane

ØKOKRIM

Regjeringsadvokaten

Allmennkringkastingsrådet

Anti-Piratgruppa og Scandinavian TV Organisations Against Piracy (STOP) v/ Advokatfirmaet Haavind Vislie

A-pressen ASA

BONO

Canal Digital Norge AS  
Datatilsynet  
Den Norske Advokatforening  
Den norske Dommerforening  
Det juridiske fakultet ved Universitetet i Bergen  
Det juridiske fakultet ved Universitetet i Oslo  
EFN (Elektronisk Forpost Norge)  
FONO - Foreningen norske plateselskaper  
Forbrukarombudet  
Forbrukarrådet  
GRAMO  
Handels- og Servicenæringens Hovedorganisasjon  
Institutt for medier og kommunikasjon  
Institutt for medievitenskap  
Institutt for rettsinformatikk  
Institutt for rettsvitenskap ved Universitetet i Tromsø  
Kopinor  
KRIPOS  
LINO  
Lovdata  
Norges Juristforbund  
Norges Markedsføringsforbund  
Norsk Forbund for Fjernundervisning  
Norsk Kabel-TV forbund  
Norsk Presseforbund  
Norsk Redaktørforening  
Norsk Rikskringkasting  
Norsk Videogramforening  
Norske film- og TV-produsenters forening  
Norske Film- og Videoprodusenters Forening, Norsk Film AS  
Norske Fjernsynsselskapers Landsforbund  
Norske Videogramhandleres forbund  
Norwaco  
Orkla Media AS  
Schibsted ASA  
Statens medieforvaltning  
Straffelovkommisjonen  
Straffelovrådet  
Tele2 Norge AS  
Telenor AS  
TONO  
TV Norge AS  
TV2 AS  
TV3 AS  
TV4 - Nordisk Televisjon AS, og  
UPC.

Høyringsfristen var 25. april 2000. Følgjande instansar hadde ingen merknader:

Barne- og familiedepartementet  
Fiskeridepartementet  
Finansdepartementet  
Forsvarsdepartementet  
Kommunal- og regionaldepartementet  
Miljøverndepartementet  
Olje- og energidepartementet  
Sosial- og helsedepartementet  
Utanriksdepartementet  
Høgsterett  
Borgarting lagmannsrett  
Regjeringsadvokaten  
Riksadvokaten (slutta seg til fråsegna frå ØKOKRIM)  
Universitetet i Tromsø  
Kripos  
Handels og Servicenæringens Hovedorganisasjon  
Norsk Videogramforening  
Forbrukarombodet  
Forbrukarrådet  
Den Norske Advokatforening, og  
Norwaco  
Følgjande instansar hadde merknader til realiteten i framlegget:  
Antipiratgruppa, herunder STOP  
Arbeids- og administrasjonsdepartementet  
BONO  
EFN (Elektronisk Forpost Norge)  
Nærings- og handelsdepartementet  
Samferdselsdepartementet  
Straffelovkommisjonen  
Statens medieforvaltning  
TONO  
ØKOKRIM

### 3 Om direktiv 98/84/EF og gjeldande norsk rett

#### 3.1 Innleiing

---

Framlegget her til endring av straffeloven § 262 tek sikte på gjennomføre direktiv 98/84/EF i norsk rett. Det er difor nødvendig å gå noko nærare inn på sjølve direktivet og gjeldande norsk rett på området.

#### 3.2 Informasjonssamfunnstenester

---

Direktivet gjev etter artikkel 2 bokstav a rettsleg vern til kringkastings- og informasjonssamfunnstenester. Sjølve omgrepet «informasjonssamfunnstenester» er ikkje godt reint språkleg, men har fått ein etablert og klar definisjon i EU/EØS-rettsleg samanheng, jf. mellom anna direktiv 2000/31/EF om elektronisk handel. Omgrepet blir derfor nytta også her.<sup>1)</sup>

Definisjonen av informasjonssamfunnstenester er gitt i artikkel 1 nr. 2 i direktiv 98/34/EF, slik dette lyder etter endringa ved direktiv 98/48/EF (i dansk versjon):

«enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

Med henblik på denne definition forstås ved

- «teleformidling»: at en tjeneste ydes, uden at parterne er til stede samtidig
- «ad elektronisk vej»: at en tjeneste fra afsendelsesstedet sendes og på bestemmelsesstedet modtages ved hjælp af elektronisk databehandlingsudstyr (herunder digital komprimering) og datalagringsudstyr, og som udelukkende sendes, rutes og modtages via tråd, radio, optiske midler eller andre elektromagnetiske midler
- «på individuel anmodning fra en tjenestemodtager»: at en tjeneste ydes ved transmission af data på individuel anmodning.»

Til definisjonen finst ei rettleiande liste over tenester som *ikkje* er omfatta av definisjonen. Dette er mellom anna:

1. Tenester som ikkje vert «teleformidlet», dvs. tenester der ein tek i bruk elektroniske innretningar men der tenesteleverandør og tenestemottakar er fysisk til stades, så som

- a) undersøking eller behandling på eit legekontor der ein nyttar elektronisk utstyr, og der pasienten er fysisk til stades,
- b) søk i ein elektronisk katalog i ei forretning, når kunden er fysisk til stades,
- c) bestilling av flybillettar via eit datanett i eit reisebyrå, når kunden er fysisk til stades, eller

---

<sup>1)</sup> I den danske direktivteksta nyttast omgrepet «informationssamfundets tjenester», på svensk heiter det «informationsamhällets tjänster», på engelsk «information society services», på tysk «Diensten der Informationsgesellschaft» og på fransk «des services de la société de l'information».

d) elektroniske spel i ein spelehall, der brukaren er fysisk til stades.

2. Tenester som ikkje blir formidla «ad elektronisk vej» fordi tenestene har eit fysisk innhald sjølv om dei inneber bruk av elektroniske innretningar, så som

- a) penge- og billettautomater,
- b) tilgang til vegnett, parkeringsanlegg osv. mot betaling, også når det ved inn- og/eller utkjøring er sett opp elektroniske innretningar for kontroll av tilgangen og/eller for å sikre rett betaling.

3. Tenester som ikkje blir formidla «ad elektronisk vej» fordi dei ikkje blir ytt via elektroniske system for datalagring eller databehandling, så som

- a) taletelefonitenester,
- b) telefax-/telextenester,
- c) tenester som vert ytt gjennom taletelefoni eller telefax,
- d) konsultasjon av lege, advokat mm. per telefon eller telefax,
- e) direkte marknadsføring per telefon eller telefax.

4. Tenester som av andre grunnar ikkje blir formidla «ad elektronisk vej», som til dømes distribusjon av CD-rom og programvare på diskett (offlinetenester),

5. Tenester som ikkje vert formidla «på individuel anmodning af en tjenestemodtager», dvs. tenester som vert ytt gjennom utsending av data men utan at det føreligg noko individuell oppmoding fordi meininga er at utsendinga skal nå fram til eit uavgrensa tal mottakarar (punkt-til-multipunkt-transmisjon), så som

- a) TV- og radioutsending (også near-video on-demand-tenester) som omhandla i artikkel 1 bokstav a i direktiv 89/552/EØF,
- b) radioutsending,
- c) tekst-TV.

### 3.3 Verksemd som skal vere ulovleg

---

I direktivet 98/84/EF vert det lagt til grunn at den digitale teknologien gjer det mogleg å gi forbrukarane fleire val, og at dette vil styrke det kulturelle mangfaldet. Det er likevel truleg slik at ei rekkje av desse tenestene berre vil bli bydde fram når tenesteytaren er sikra eit vederlag. Dette vert i praksis gjennomført ved hjelp av ulike former for tilgangskontroll (autorisasjon).

For å verne om retten til å innkassere vederlag for slike tenester må leverandørane ha eit vern mot utstyr og programvare som kan gi gratis tilgang. Direktivet inneheld difor eit forbod mot forretningsdrift knytt til utstyr som gir slik ulovleg tilgang. Etter artikkel 4 skal medlemsstatane forby framstilling, import, distribusjon, sal, utleige, innehaving, installering, vedlikehald, utskifting og marknadsføring av slikt utstyr med kommersielt formål.

Det er opp til den enkelte medlemsstat å avgjere om det i tillegg skal legast ned forbod mot privat innehaving og bruk av ulovleg utstyr, jf. fortalen punkt 23.

Direktivet krev at medlemsstatane skal ha ei intern lovgjeving som gir dei som yter verna tenester, tilgang til høvelege rettsmiddel for å stanse og avbøte ulovleg spreiding mm. av piratutstyr eller piratprogramvare, jf. artikkel 5. Mellom anna skal det være mogleg å be om mellombels rådgjerd, gå til skadebotsøksmål, og eventuelt be om at dei ulovlege innretningane vert fjerna frå

handelen. Direktivet krev ikkje at brot på desse reglane skal vere straffbart, men set heller ikkje forbod mot at straff vert nytta.

### 3.4 Særleg om vederlagsinteressen

---

Siktemålet med direktivet er å verne *vederlaget* for dei tenestene som direktivet gjeld. Tilgangskontroll gjennom ulike former for koding og kryptering mm. må derfor ha eit økonomisk motiv for å være omfatta av direktivet. Dette vil til dømes normalt være tilfelle for ei teneste som videogram på bestilling. For slike tenester vil vederlaget vere ein føresetnad for tilbodet av tenesta og utsiktene til økonomisk forteneste vil vere sjølv motivet for at tenesta blir bydd fram.

Denne avgrensinga er tatt inn i direktivet for å unngå at direktivet vert gjeldande for tenester som fell utanfor føremålet med reguleringa, som t.d. bankane sine automatiske kontotelefonar og mobiltelefonar der det er brukt PIN-kodar. Desse tenestene er ikkje koda av omsyn til eit vederlag, men av omsyn til kundane sin tryggleik. Også andre grunngjevingar for å kontrollere tilgang, så som vern av åndsverk eller vern av mindreårige mot mogleg skadeleg innhald, fell utanfor.

Vidare må den ulovlege aktiviteten ha eit kommersielt føremål. Dette inneber at direktivet ikkje krev forbod mot førebuande handlingar eller andre aktivitetar med sikte på privat bruk. Å leggje programvare mm. gratis ut på ei web-side utan at det skjer med sikte på forretningsverksemd, vil ikkje vere ei ulovleg handling etter direktivet, og heller ikkje det å laste ned verna informasjon frå nettet dersom dette berre er til privat bruk.

### 3.5 Gjeldande rett på området

---

Om gjeldande rett på området er det sagt følgjande i høyringsnotatet:

#### «3.1 Straffeloven

Etter gjeldende straffelov § 262 er det forbudt «ved å bryte en beskyttelse eller på lignende måte» å skaffe seg selv eller andre «en vinning ved å få tilgang til fjernsyns- eller radiosignaler». Også medvirkning er gjort straffbart.

Bestemmelsen innebærer dermed en beskyttelse for krypterte og kodete kringkastingssendinger. Formuleringen «fjernsyns- og radiosignaler» dekker etter sin ordlyd mer enn dette idet mange informasjonssamfunnstjenester også formidles ved hjelp av fjernsyns- og radiosignal. Bestemmelsens forarbeider (Ot.prp. nr. 4 (1994-95) bl.a. s. 49 første spalte og s. 52 første spalte) viser imidlertid at bestemmelsen tok sikte på kringkastingssendinger, jf. definisjonen av kringkasting i kringkastingsloven 4. desember 1992 nr. 127 § 1-1 første ledd:

«Med kringkasting menes utsending av tale, musikk, bilder og liknende med radiobølger eller over tråd, ment til å mottas direkte av allmennheten».

For at en tjeneste skal anses som kringkasting er det et vilkår at sendingene er ment for allmennheten. Dette vilkåret oppfylles ikke av f.eks. tjenesten videogram på forespørsel, fordi det enkelte program ikke sendes ut til en allmennhet, men på bakgrunn av en individuell bestilling.

Straffeloven § 145 annet ledd gjør det straffbart «ved å bryte en beskyttelse eller på lignende måte uberettiget» å skaffe seg adgang til «data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske midler». Også medvirkning er gjort straffbart.

Ved to avgjørelser fra Høyesterett (Rt. 1994 s. 1610 og Rt. 1995 s. 35) er det avklart at begrepet «data» ikke omfatter fjernsynsprogrammer. Det er uttalt at det rent språklig er naturlig å forstå uttrykket «data» slik at det omfatter «faktiske opplysninger og informasjon», jf. Rt. 1994 s. 1612.

Det er etter dette liten grunn til å anta at informasjonssamfunnstjenester som videogram på forespørsel vil være dekket av begrepet «data». At videogram på forespørsel er disponibel etter individuell bestilling mens kringkasting er rettet mot en allmennhet (abonnentene som sådanne), kan vanskelig begrunne en løsning hvor den ene tjenesten dekkes av databegrepet i straffeloven § 145 annet ledd mens den andre (kringkasting) ikke gjør det. Det er derfor grunn til å anta at § 145 ikke rammer all den virksomhet som reguleres i direktivet.

Konklusjonen må derfor bli at verken straffeloven § 262 eller straffeloven § 145 annet ledd fullt ut dekker de kravene til forbud som følger av direktiv 98/84/EF.

### 3.2 Markedsføringsloven

Også markedsføringsloven (lov 16. juni 1972 nr. 47) § 1 første ledd dekker deler av de forhold som omtales i direktivet. Bestemmelsen lyder:

«I næringsvirksomhet må det ikke foretas handling som strider mot god forretningsskikk næringsdrivende imellom, eller er urimelig i forhold til forbrukere eller som for øvrig strider mot god markedsføringsskikk.»

Begrepet handling omfatter klart nok aktiviteter som salg, utleie og markedsføring, og slike handlinger - utført i næringsvirksomhet - vil stride mot god forretningsskikk dersom siktemålet er å gi kundene tilgang til kodete tjenester uten at det betales vederlag for tjenesten til rettighetshaveren.

En rent språklig forståelse av begrepet handling vil også omfatte aktiviteter som vedlikehold, installasjon og utskiftning. I praksis er det vel likevel tvilsomt om en slik tolkning vil bli lagt til grunn. Forarbeidene omtaler ikke forholdet nærmere og bestemmelsenes generelle karakter kan tale for en innskrenkende tolkning med hensyn til handlingens art. Ut over omsetning (salg, leie, produksjon etc.), er det begrenset domspraksis relatert til det å opprette eller bidra til å opprette ulovlig tilgang til beskyttede tjenester.

Departementet legger derfor til grunn at bestemmelsen ikke i tilstrekkelig grad dekker forpliktelsene etter direktiv 98/84/EF med hensyn til handlinger som vedlikehold, reparasjon og utskiftning av innretninger som gir tilgang til kodete tjenester uten rettighetshaverens samtykke, jf. direktivet art. 4 bokstav b.

### 3.3 Åndsverkloven

Der tilgangsstyrte og tilgangsstyrede tjenester sprer, viser eller framfører et åndsverk som nevnt i åndsverkloven (lov 12. mai 1961 nr. 2) § 1 annet ledd, vil verket ha et selvstendig vern etter åndsverklovens regler. Overtredelse av lovens bestemmelser til vern om åndsverk er straffesanksjonert.

Det vernede objekt etter åndsverkloven er imidlertid et annet enn det som oppstilles i direktivet om beskyttelse av kodete tjenester. Verket etter åndsverkloven er et vern mot uautorisert utnyttelse av inn-

hold (dvs. åndsverket), mens direktivet gir et vern mot at noen skaffer seg tilgang til innholdet, gjennom å fjerne adgangssperrer.

Åndsverkloven § 54a gjelder bare innretninger som verner data-maskinprogram, og oppfyller derfor heller ikke direktivets krav.

Det er vedtatt to nye internasjonale traktater på opphavsrettsområdet - innenfor organisasjonen World Intellectual Property Organization (WIPO) - som gir regler om beskyttelse av adgangssperrer som har til formål å hindre uautorisert utnyttelse av åndsverk/lignende arbeider.

<sup>2)</sup> Disse traktatene vil Norge tiltre. Også innen EU arbeides det med et direktivforslag om opphavsrett som også inkluderer forpliktelser mht. vern mot uautorisert fjerning av slike adgangssperrer som drøftes her.

<sup>3)</sup>

### 3.4 Tilgang til rettsmidler

Departementet mener direktivets art. 5 nr. 2 om at tilbydere av kodede tjenester skal ha tilgang til passende rettsmidler når de påføres skade, vil bli fullt ut dekket ved en vedtakelse av den lovendringen som her foreslås. Dette gjelder også adgangen til å anlegge erstatnings-søksmål, under henvisning til at handlinger som er straffbare også er sivilrettslig forbudt.

Departementet anser adgangen til midlertidig forføyning etter tvangsfullbyrdelsesloven kapittel 15 for å tilfredsstille direktivets krav om at det skal kunne anvendes «foreløbige rettsmidler», jf. dansk versjon av direktivet. I den norske oversettelsen brukes begrepet «forebyggjande tiltak», som vel må betraktes som en oversettelsesfeil.»

Det følger av det som er sagt ovanfor om direktiv 98/84/EF at ikkje alle dei materielle sidene ved direktivet er gjennomførte i norsk rett, korkje i privatretten eller i strafferetten. Dette gjer det nødvendig å gjere framlegg om lovendringar.

---

<sup>2)</sup> WIPO Copyright Treaty (CRNR/DC/94) og WIPO Performances and Phonograms Treaty (CRNR/DC/95), begge vedtatt 20. desember 1996.

<sup>3)</sup> Forslag til Europa-Parlamentets og Rådets direktiv om harmonisering af visse aspekter as ophavsret og beslægtede rettigheder i informationssamfundet (98/C108/03) KOM(97) 628.

## 4 Nordisk rett

Direktivet er gjennomført på ulikt vis i dei andre nordiske landa.

I *Danmark* følger det av § 75 a i «lov om radio- og fjernsynsvirksomhed» at det er forbode å framstille, importere, omsette, inneha eller endre dekodrar og anna dekodingsutstyr «hvis formål det er» å gi uautorisert tilgang til innhaldet i ei koda radio- eller fjernsynsutsending. Fram til lov 31. mai 2000 råka dette berre slike handlingar når dei hadde «erhvervsmæssigt øjemed». Dette vilkåret vart då fjerna, med blant anna det resultat at det i Danmark no er ulovleg å inneha slike innretningar også reint privat. Etter same paragraf er også annonsering og anna form for reklame for slike innretningar forbode.

Dersom aktivitetane «finder sted i erhvervsmæssigt øjemed» er straffa bøter eller fengsel opp til 6 månader. Utanfor ein slik samanheng kan ein berre dømast til bøter. Den høgare strafferamma gjeld likevel for utbreiing til ein vidare krets, sjølv om dette ikkje skjer som ledd i næringsverksemd. Det er i lovframlegget sagt at dette særleg tek sikte på spreiding av passord, kodar o.l. via internett. Skuldkravet er i alle tilfelle grov aktløyse eller forsett.

I *Sverige* er spørsmålet regulert i lov 2000:171 om «förbud beträffande viss avkodningsutrustning», som avløyste lov 1993:1367 «om förbud beträffande viss avkodningsutrustning (avkodningslagen)». Den nye lova kom som ei direkte følgje av direktiv 98/84/EF. Lova inneheld 10 paragrafar, noko som kanskje har gjort det mogleg med ei meir oversiktleg regulering enn det vi kan få til i norsk rett, når alt skal inn i berre ein paragraf i straffeloven.

Den svenske lova dekkjer både radio, fjernsyn, informasjonssamfunnstenester (forklart som « varje annan tjänst som utförs elektroniskt, på distans och på begäran av mottagaren») og sjølvle tilgangskontrollen til slike tenester når denne må oppfattast som ei eiga teneste.

Tilgangskontroll er definert i 3 § på følgjande måte:

«Med villkorad tillgång till en tjänst avses att en användare eller en mottagare av tjänsten till följd av tekniska åtgärder eller arrangemang kan få tillgång till tjänsten i tolkningsbar form först sedan de har blivit personligt godkända som behöriga.»

Sjølvle forbodet finst i 5 § første ledd, der det heiter at «Avkodningsutrustning får 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.»

Føreseigna ligg tett opptil direktivet artikkel 4. Mellom anna følgjer av dette at korkje privat bruk eller det å inneha er gjort straffbart. Strafferamma er bøter eller fengsel i høgst to år.

I *Finland* finn ein dei viktigaste reglane om koda tenester i telemarknadslagen (lov 396/1997). Dekodarsystem er her definert som (4 § p. 22):

«en utrustning, en del av utrustning eller ett annat system vars ändamål är att koppla bort skyddet för ett i telenätet förmedlat meddelande som skyddas med hjälp av ett särskilt tekniskt system».

Sjølve forbudet finn ein i 25 § første mom., som lyder:

«Det är förbjudet att orättmätigt inneha, använda, tillverka, importera eller främja försäljningen av dekodningssystem.»

Dette inneber at også det å inneha privat er straffbart, men etter det departementet kjenner til er dette spørsmålet for tida oppe til ny vurdering. Strafferamma for brot på 25 § er bøter.

## 5 Framlegget i høyringsnotatet

### 5.1 Framlegg til lovtekst

---

I høyringsnotatet 1. mars 2000 gjorde Justisdepartementet framlegg om at straffeloven § 262 skulle lyde:

«Den som med kommersielt formål

- a) framstiller, innfører, distribuerer, selger, leier ut eller besitter ulovlig dekodingsutstyr,
- b) installerer, vedlikeholder eller skifter ut ulovlig dekodingsutstyr, eller
- c) formidler eller markedsfører ulovlig dekodingsutstyr,

eller medvirker til dette, straffes med bøter eller fengsel inntil 1 år. På samme måte straffes den som utbrer ulovlig dekodingsutstyr til en videre krets.

Den som rettsstridig skaffer seg selv eller andre en vinning ved bruk av ulovlig dekodingsutstyr straffes med bøter.

Med ulovlig dekodingsutstyr menes i denne paragraf teknisk utstyr, programvare, koder, kodenøkler eller passord som gir tilgang i forståelig form til

- a) fjernsyns- eller radiosignaler, eller
- b) tjenester som ytes mot vederlag og som teleformidles elektronisk på anmodning fra den enkelte tjenestemottaker (informasjonssamfunnstjenester),

uten tillatelse fra rettighetshaveren.

Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale.»

### 5.2 Grunngeving for framlegget

---

I grunngevinga for framlegget viste departementet til at vern av koda tenester i vårt land i hovudsak er gjennomført ved føresegner i straffeloven. Ein såg ikkje grunn til å gå vekk frå dette.

Det vart vidare vist til Straffelovrådet sine lovtekniske drøftingar i NOU 1985: 31 Datakriminalitet, departementet sine drøftingar i Ot.prp. nr. 35 (1986-87) om endringer i straffeloven (datakriminalitet) og justiskomiteen sine drøftingar i Innst. O. nr. 66 (1986-87). I sistnemnde dokument er det uttalt at reglane mot «datakriminalitet» ikkje bør samlast i eit eige kapittel i straffeloven, men heller bli arbeidd inn i gjeldande aktuelle føresegner «idet beslektede tilfeller bør behandles mest mulig likt uavhengig av hvilken framgangsmåte som er benyttet ved lovovertrædelsen», jf. Innst. O. nr. 65 (1986-87) s. 3 første spalte.

I høyringsbrevet er det og vist til at Straffelovkommisjonen arbeider med kapittelstrukturen i straffeloven, men at departementet - fram til dette arbeidet

eventuelt gir nye retningslinjer - vil foreslå at mindre lovrevisjonar vert tekne inn i eksisterande føresegner.

I høyringsbrevet stilte departementet spørsmål ved om direktivet var omfattande nok. Det var vist til at ulovleg dekodarutstyr, medrekna programvare, kodar og passord, i dag vert distribuert på ein slik måte at svært lite vil bli fanga opp av gjerningsskilddringa i artikkel 4, jf. definisjonen av «ulovleg innretning» i artikkel 2 bokstav e.

Dette var forklart slik:

«Det tekniske utstyret (hardwaren) som er nødvendig for urettmessig tilgang til betalingstjenester vil normalt være legalt, bl.a. fordi dette er elektronisk utstyr som har andre og klart legale bruksområder. Det er først når legalt utstyr kobles med passord, koder, kodenøkler, programmerte smartkort etc. at man får den utrustningen som er nødvendig for urettmessig tilgang til betal-TV, betal-radio og informasjonstjenester. Mens enkelte forhandlere tidligere omsatte ferdig programmert piratutstyr, selges det i dag helst lovlig elektronikk som kunden selv gjør om til piratutstyr. Kunnskap om hvordan dette skal gjøres og hvilke koder som skal benyttes finnes på flere internett-sider. Det er antydning at enkelte forhandlere - som vet eller antar at kunden ønsker å bruke elektronikken på urettmessig måte - opplyser om aktuelle internettadresser. Men selv uten slik medvirkning fra forhandleren er kunnskap om disse sidene lett tilgjengelig i ulike piratmiljøer.

Direktivet omfatter ikke kommersiell omsetning m.v. av legalt elektronisk utstyr som først blir omgjort til piratutstyr av sluttbrukeren. Etter definisjonen i art 2 bokstav e er «ulovleg innretning» utstyr og programvare «som er utforma eller tilpassa» for å gi tilgang i forståelig form uten tillatelse fra rettighetshaveren. Det omfatter ikke utstyr som kan utformes eller tilpasses, gitt at man har tilgang til nødvendige koder etc. Slik kan bestemmelsen heller ikke utformes idet den da ville omfatte elektronikk med en rekke lovlige bruksområder. Det ville på sett og vis bli som å kriminalisere omsetning av kopimaskiner med den begrunnelse at de også kan benyttes til kopiering i strid med åndsverkløven.

Departementet mener straffeloven § 262 bør utformes slik at den rammer de mest straffverdige formene for ikke-kommersiell spredning av piratutstyr og pirat-know how. Beskrivelsen foran av hvordan lovlig elektronikk kombineres med «ulovlige» koder etc. hos sluttbrukeren, viser at direktivet ikke gir tilbyderne av de aktuelle betalingstjenestene godt nok vern. Departementet foreslår derfor at definisjonen av «ulovlig dekodingsutstyr» (i direktivet «ulovleg innretning») gjøres mer omfattende. I tillegg til utstyr og programvare foreslås inntatt «koder», «kodenøkler» og «passord», jf. lovforslaget fjerde ledd. Dette vil bl.a. dekke kryptoalgoritmer, PIN-koder og Content Scrambling System (CSS), men også kommende krypteringssystem som etter en naturlig språklig forståelse vil være en kode, en kodenøkkel eller et passord.

I tillegg foreslås det at utbredelse av ulovlig dekodingsutstyr til en videre krets gjøres straffbart uavhengig av om gjerningsmannen gjør dette med kommersielt formål eller om dette gir gjerningsmannen eller andre en rettsstridig vinning, jf. lovforslaget annet ledd. Dette vil typisk ramme den som urettmessig gjør en kode kjent via internett.

Det kunne i tillegg være aktuelt å kriminalisere selve det å knekke en kode. Konsekvensene av et slikt forbud er imidlertid svært usikre,

og kan komme i strid med f.eks. åndsverkloven §§ 39h og 39i, samt prinsippene om retten til «omvendt utvikling» («reverse engineering»). Sistnevnte rettighet må antas å ha vært viktig i utviklingen av stadig ny datateknologi.»

## 6 Merknader frå høyringsinstansane og departementets vurdering

### 6.1 Innleiing

---

Ingen av høyringsinstansane er avvisande til at direktiv 98/84/EF vert gjennomført i norsk rett ved ei endring i straffeloven § 262, slik det vart gjort framlegg om i høyringsbrevet. Det er heller ikkje framsett innvendingar mot at føresegna vert omdisponert. Tvert om er det stor prinsipiell tilslutning til lovframlegget. Berre *EFN* (Elektronisk Forpost Norge) melder ein generell skepsis til framlegget, og uttaler m.a. at det er «vanskelig å trekke en annen slutning enn at den foreslåtte lovendring kan sees på som et første trinn i en prosess for sterkt å øke eiernes rettigheter, og derav redusere brukernes - menneskehetens - rettigheter i forhold til adgang til åndsverk».

Sjølv med klar tilslutning til framlegget, har fleire høyringsinstansar innvendingar mot einskilde delar av utkastet i høyringsbrevet. Desse innvendingane blir drøfta her.

### 6.2 Behov for allmenne reglar mot uautorisert tilgang?

---

Einskilde høyringsinstansar peiker på behovet for allmenne reglar mot uautorisert tilgang til digitalisert informasjon, anten dette er «on line»-tenester eller «off line»-tenester. Det vert vist til at direktiv 98/84/EF - og departementets framlegg - berre gjeld kringkastingssignal og «on line»-tenester, slik at t.d. eit leksikon på CD-rom eller ein film på DVD-plate, sjølv om dei har tilgangsvern, ikkje er omfatta. Desse «off line»-tenestene kan derimot - etter tilhøva - vere verna etter straffeloven § 145 andre ledd. *ØKOKRIM* seier m.a. om dette:

«Det er nødvendig å behandle digitalisert tilgangsbeskyttet informasjons likt, uavhengig av innholdet. Man bør kanskje opprettholde den nåværende inndelingen, slik at § 262 beskytter vederlagsinteressen bak tilgangskontrollerte «on line» tjenester, mens § 145 annet ledd bør ivareta sikkerhets- og konfidensialitetshensyn, dv. verne om brudd på tilgangskontroll satt til vern av datasystemer.

Dertil er det behov for en avklaring vedrørende den strafferettslige beskyttelse til tilgangskontrollerte «off line» tjenester som selges mot vederlag og ofte på spesielle lisensbetingelser. Her er sammenhengen mellom misbruk og krenkelse av vederlagsinteressen umiddelbart mye mindre enn for «on line» tjenester, siden rettighetshaveren uansett har fått solgt et eksemplar av sitt produkt. Ved krenkelse av beskyttelsen til «on line» tjenester går jo leverandøren glipp av vederlaget i sin helhet. Trusselen for rettighetshaverne til «off line» tjenester er imidlertid at kjøperne bryter kopieringsbeskyttelsen, dvs ikke bare skaffer seg lesetilgang men også kopieringstilgang. Påfølgende viderekopiering/spredning av den digitaliserte informasjonen kan undergrave markedet for leverandøren.

Disse spørsmål blir stadig oftere satt på prøve, og lovgiveren har all mulig grunn til å [ta] dem opp til snarlig vurdering.»

Også *TONO* er opptatt av at det vil vere uheldig om vi får ulik straff for tilnærma like brotsverk. Organisasjonen ønskjer at same føresegn skal dekkje både det å knekkje koden på ein fysisk kjøpt DVD-film og det å bryte krypteringa på den same filmen levert på bestilling gjennom nettet. Det heiter vidare:

«TONO vil derfor foreslå at departementet ser nærmere på konsekvensen av forholdet mellom forslaget til ny straffelovsbestemmelse § 262, og den svært begrensede bestemmelsene i åndsverkloven som regulerer tilgangskontroll, jfr. § 54a), samt strl. § 145, 2. ledd, slik at formålet med reguleringen og innarbeidelse av direktivet allerede nå kan bli et effektivt redskap og gi et strafferettslig vern av innhold, uansett om dette er utformet som en kryptert betalingstjeneste, datamaskinprogram eller som et rent beskyttet åndsverk.»

Departementet er klar over at framlegget til strl. § 262 ikkje vil fange opp alle sider knytt til uautorisert tilgang til tilgangskontrollert digitalisert informasjon. I denne omgang er det likevel ikkje aktuelt å ta opp anna enn dei sidene ved dette som alt er regulert i strl. § 262 og det som er omhandla i direktivet, dvs. vern av vederlaget til tenesteytarane ved «on line»-tenester. Å kome med framlegg om ei meir samla lovgjeving om digital informasjon vil vere ein naturleg del av arbeidet i Straffelovkommisjonen.

### 6.3 Kva for tenester bør vere verna?

---

Ingen av høyringsinstansane, med unntak av den generelle skepsisen ein finn hjå EFN, har negative kommentarer til at vernet i § 262 vert utvida frå «fjernsyns- og radiosignal» til å omfatte også det som i direktivet er kalla informasjonssamfunnstenester. *BONO* peikar på at det er nødvendig å utvide vernet til informasjonssamfunnstenester «tatt i betraktning den teknologiske utvikling hvor de ulike medier i stor grad konvergerer. En medienøytral lovgivning er viktig for å unngå en situasjon hvor likeartede tjenester behandles forskjellig».

Det er ikkje kome merknader til at sjølve tilgangskontrollen skal vere omfatta der dette er å sjå på som ei eiga teneste.

I høyringsbrevet gjorde departementet framlegg om å nytte omgrepet informasjonssamfunnstenester i sjølve lovteksta. *Arbeids- og administrasjonsdepartementet* uttaler om dette at ein ikkje er «sikre på om begrepet «informasjonssamfunnstjenester», slik det er definert i EU, bør innføres i norsk lovgivning. I så fall burde definisjonen kunne modifiseres slik at den gjenspeilet den teknologiske utviklingen bedre».

Departementet er ikkje usamd i dette og har no tatt ut omgrepet frå lovframlegget. Definisjonen av dei verna tenestene står godt nok på eigne bein utan at ordet «informasjonssamfunnstenester» vert nytta.

*Økokrim* ber om at det vert tatt stilling til om dei frie rikskanalane, som NRK, NRK2 og TV2, skal vere omfatta. Desse sendingane er koda når dei vert sende via satellitt, men ein kan dekode signala på lovleg vis ved bruk av såkalla «Satellittkort», som vert selde av autoriserte forhandlarar. *Økokrim* forklarar problemet slik:

«Det er selvsagt mulig å bruke piratdekoderkort i stedet for Satellittkort. Kodene til rikskanalens sendinger er tilgjengelige på Internett og det er ikke uvanlig at piratene koder kortene slik at hvert kort gir til-

gang til flere kanaler, både betalings-TV-tjenester og rikskanalene. Uansett om man bor i et område hvor rikskanalene har ordinær dekning eller ei, er det nødvendig å kode kortene med flere kanaler for å kunne benytte fjernkontrollen. Hvis ikke må brukeren bytte kort ved hvert kanalskifte.

Vi antar at intensjonen er at rikskanalene ikke skal være omfattet av § 262, siden de ikke hører til de vanlige betalings-TV-konseptene. På den annen side taler sterke prosessøkonomiske hensyn for at de blir omfattet. Erfaringsmessig vil siktede påberope seg at han vesentlig har solgt piratdekoderkort for at kundene skal se rikskanalene, dvs kanaler som han allerede har betalt for via TV-lisensen og som det derfor ikke umiddelbart er naturlig å ramme ved bruk av § 262. Dette har skapt problemer ved anvendelsen av § 262, både om straffeskylden og omfanget av overtredelsen.»

D e p a r t e m e n t e t har forståing for dei bevisproblem som Økokrim her syner fram. Det kan likevel ikkje vere eit godt nok argument til å la føresegna omfatte signal frå opne rikskanalar. Ein bør for systematikken si skuld halde fast ved at berre tenester som er tilgangskontrollerte av omsyn til vederlaget er omfatta. Departementet er ikkje kjent med årsaka til at dei elles frie signala frå rikskanalane er koda når dei kjem via satellitt, men legg til grunn at dette i alle fall ikkje er gjort for å verne eit vederlag. Det er heller ikkje naturleg å sjå det slik at den som ved sal av «piratkort» skaffar nokon tilgang til satellittkanalar som er ope tilgjengelege i det jordbundne nettet, medverkar til uautorisert tilgang, når kodinga har ei teknisk grunngeving, og ikkje er eit tiltak for å sikre leverandøren betaling for tenesta si.

D e p a r t e m e n t e t har vurdert om omgrepet «fjernsyns- og radiosignal» i gjeldande § 262 bør bli bytta ut med «kringkasting», jf. lov 4. desember 1992 nr. 127 om kringkasting § 1 første ledd, eller om det ville vere tenleg å nytte definisjonane i direktivet artikkel 2 (a). Då departementet ikkje kan sjå at bytte av omgrep vil gi føresegna noko anna innhald, har ein kome til at det ikkje er nødvendig med endringar her.

*Statens medieforvaltning* har merka seg at departementet i framlegget «benytter begrepene «teleformidling» og «elektronisk» i stedet for begrepet «telekommunikasjon» slik dette er definert i telelovens § 1-6». Statens medieforvaltning har likevel ikkje motsett seg dette, og departementet finn det difor best å halde fast ved desse omgrepa, som også språkleg høver best. Innhaldet i «elektronisk teleformidling» er likevel det same som i «telekommunikasjon» etter teleloven.

#### **6.4 Kva for innretningar for dekodning skal vere omfatta?**

---

I høringsnotatet nytta departementet omgrepet «ulovleg dekodingsutstyr» om dei tilgangskontrollerande innretningane. Høringsrunden har vist at dette omgrepet ikkje er heilt godt.

For det første har nokre høringsinstansar, m.a. *Samferdsledepartementet* peika på at «utstyr» gir for klare assosiasjonar til «noe man fysisk kan ta på, mens dette nødvendigvis ikke er tilfellet». I staden blir foreslått «innretning» eller «anordning».

For det andre blir det peika på at omgrepet må vere teknologinøytralt for å vere tilpassa framtidig teknologi. *Arbeids- og administrasjonsdepartementet* meiner m.a. av den grunn at «innretning» er betre egna enn «utstyr».

*D e p a r t e m e n t e t* er samd i dette. Det sentrale er å finne fram til eit omgrep som femner om det ein er ute etter: Omgrepet skal dekke alle hjelpemiddel, anten dette er utstyr (hardware) eller programvare (software), som er utforma eller tilpassa - åleine eller saman med andre hjelpemiddel - for å gi tilgang i forståeleg form til ei verna teneste. Samstundes må omgrepet ha slike kvalitetar at ein ved første gongs lesing får eit rimeleg inntrykk av kva ein siktar til. Det beste omgrepet departementet har funne, som dekker desse krava, er «dekodarinnretning» (i lovteksta på bokmål: «dekodingsinnretning»).

Testen på om noko er ei dekodarinnetning etter denne definisjonen, vil vere om utstyret eller programvara, åleine eller saman med andre hjelpemiddel, kan gi tilgang i forståeleg form til ei verna teneste. Definisjonen er knytt opp til funksjonen til det aktuelle hjelpemiddel. Nye, framtidige innretningar for tilgangskontroll - som vi per i dag ikkje kjenner til - vil difor også bli råka om innretningane har dei omtala eigenskapane.

I høringsbrevet foreslo departementet å ta inn omgrepa «kode», «kode-nøklar» og «passord» i tillegg til utstyr (hardware) og programvare (software). Dette var meint som døme på aktuelle innretningar. Fleire høringsinstansar meinte dette ville skape meir forvirring enn avklaring, og somme såg dette som ei utviding i høve til direktiv 98/84/EF.

*J u s t i s d e p a r t e m e n t e t* kan ikkje vere samd i at dette er ei utviding i høve til direktivet. Kodar, kodenøklar og passord vil normalt vere innretningar som har dei eigenskapane som etter definisjonen konstituerer ei dekodarinnetning.

Slik har også dette blitt forstått av *Arbeids- og administrasjonsdepartementet*, som uttaler: «Krypteringssystem dekkes svært godt av begrepene «utstyr» og «programvare», da dette implementeres nettopp ved hjelp av disse. «Koder» og «kodenøkler» som det refereres til, legges som regel i et smartkort - altså utstyr (hardware), dvs. disse begrep dekkes av dette».

Det same departementet er derimot ikkje samd i at «utstyr» og «programvare» vil dekkje t.d. PIN-kodar: «PIN-kode er en *personlig* tilgangskode (Personal Identification Number). Utlekking av slike på Internett vil ramme innehaveren av koden og ikke leverandøren av betalbare tjenester, slik vi ser det. Vi vil derfor stille oss tvilende til behovet for å utvide begrepet «ulovlige innretninger» slik det her foreslås.»

Til det er å seie at også PIN-kodar kan ha slike eigenskapar at dei gir tilgang til ei verna teneste. Då vil PIN-koden vere ei dekodarinnetning. Derimot vil det vel i dei fleste tilfelle vere slik, som *Arbeids- og administrasjonsdepartementet* peiker på, at rekninga for urettmessig bruk går til «eigaren» av PIN-koden. Om leverandøren av ei verna teneste får sitt vederlag også når PIN-koden blir brukt av andre enn «eigaren» av koden, vil spreiding mm. av slike kodar ikkje bli råka av § 262 første ledd. Dette fordi vilkåret om uautorisert tilgang ikkje er oppfylt.

Urettmessig *bruk* av PIN-kodar kan derimot bli råka av andre ledd, om brukaren skaffar seg sjølv eller andre ei urettmessig vinning, eller om bruken påfører «den berettigede» eit tap.

For det tredje er det ikkje tenleg å ta inn vilkåret «ulovleg» i sjølve definisjonen. Ofte kan ein ikkje avgjere berre ved å sjå på den aktuelle innretninga om ho er *lovleg* eller *ulovleg*. Dette kjem av at mange innretningar kan nyttast både til legale og illegale aktivitetar. Definisjonen må difor omfatte alle innretningar som *kan* dekode eller på annan måte gi tilgang til verna tenester, også dei legale hjelpemiddel som nokon omset eller nyttar etter autorisasjon frå tenesteleverandør. Om innretningar som også har legale bruksområder er piratutstyr eller ikkje, kan ein først avgjere etter at ein har undersøkt om det finst avtaler eller andre omstende som gjer spreiding og/eller bruk legalt eller illegalt.

Det er problematisk at mange av innretningane kan ha både eit legalt og eit illegalt bruksområde. Det fører med seg at den subjektive målsettinga bak dei ulike spreidingsaktivitetane blir avgjerande for om handlingane er lovlege eller ikkje, når innretningane har fleire funksjonar. Dette kan gi vanskelege bevisproblem for påtalemakta. Det bør tenesteleverandørane merke seg, slik at dei så langt råd er finn fram til tilgangskontrollerande innretningar som ikkje har fleire funksjonsområde. Departementet legg til grunn at bransjen sjølv ynskjer eit effektivt vern mot piratverksemd, og då bør bransjen sjølv bidra ved m.a. å velje mest mogleg unike system for tilgangskontroll.

*Antipiratgruppa* og *TONO* er kritiske til at det i framlegg til definisjon av dekodarinnettningar heiter at dette gjeld innretningar «som gir tilgang». Antipiratgruppa seier om dette:

«Etter vårt skjønn vil det kunne oppstå uheldig bevisproblemer ved at bestemmelsen krever at utstyret, for å anses som ulovlig, må gi tilgang til betalingstjenester. Det avgjørende bør etter vårt skjønn være hva som er formålet eller hensikten med utstyret, jf. den svenske og danske lovteksten. Særlig ved salg av hardware - hvor utstyret som regel vil ha andre legale anvendelsesområder - kan det tenkes at det vil kunne være enklere å bevise at ulovlig salg har funnet sted dersom formålet eller hensikten med utstyret er avgjørende.»

Departementet er samd i desse innvendingane, og gjer no framlegg om å endre dette til innretningar som er utforma eller tilpassa «for å gi tilgang». Då kjem det klart fram at det er målsettinga med innretningane som er avgjerande.

## 6.5 Nærare om uautorisert tilgang

---

I lovframlegget i høyringsbrevet hadde Justisdepartementet teke inn vilkåret «uten tillatelse fra rettighetshaveren», jf. fjerde ledd i.f.. Fleire høyringsinstansar har merknader til dette, m.a. viser *Arbeids- og administrasjonsdepartementet* til at «begrepet *kan* tolkes som opphavsrettshaveren, særlig i forhold til informasjonssamfunnstjenester, og det er vel ikke dette forholdet man skulle ramme her?».

Med den omdisponeringa som departementet no har gjort av paragrafen - m.a. er «dekodarinnettningar» og «verna teneste» definert i kvart sitt ledd -

treng ein ikkje lenger dette omgrepet. Det ein tidlegare meinte å få fram med ordlyden «uten tillatelse fra rettighetshaveren», blir no fanga opp av omgrepet «uautorisert tilgang» i første og andre ledd.

## 6.6 Dei straffbare aktivitetane

---

Ingen av høyringsinstansane har spesielle kommentarer til opprekninga av dei ulovlege handlingane, slik dette kom fram i utkastet til § 262 første ledd i høyringsbrevet. Dette er dei aktivitetane som er nemnd i direktivet artikkel 4, og som rettar seg mot bakmenn med økonomisk motiv.

*Straffelovkommisjonen* sluttar seg til framlegget om at fokus i føreseigna «bør dreies over mot distributørene», fordi det er «åpenbart at det i første rekke er distributørene man bør slå ned på».

I direktivet - og i vårt framlegg i høyringsbrevet - heiter det at desse aktivitetane berre blir råka når dei vert utført med kommersielt føremål. Somme instansar har hatt merknader til dette kravet. *ØKOKRIM* uttaler:

«Det er mulig at uttrykket «kommersielt formål» ikke er ment å legge spesielle føringer utover et krav til omfang og profittmotiv. I så fall vil første ledd helt overlappe annet ledd og skape betydelige problemer ved straffutmålingen. Det antas å være hensiktsmessig med noen klargjørende bemerkninger fra departementets side i tilknytning til det endelige lovforslaget.»

Etter ei nærare vurdering har d e p a r t e m e n t e t kome til at «vinnings hensikt» er eit betre kriterium, m.a. fordi dette allereie har eit kjent innhald, jf. nærare i kapittel 8.2.

I høyringsbrevet gjorde Justisdepartementet framlegg om visse utvidingar i høve til direktivet. Dette gjaldt straff for ikkje-kommersiell spreiking til ein vidare krets (i framlegget i høyringsbrevet var dette omhandla i andre ledd, men er no teke inn som første ledd bokstav c) og straff ved rettsstridig vinning ved bruk av piratinnretningar (i framlegget omhandla i tredje ledd, no teke inn som andre ledd). Det siste er likevel ikkje ei utviding i høve til gjeldande § 262 med omsyn til fjernsyns- og radiosignal.

Begge desse utvidingane er i hovudsak godt mottekne, om ein ser vekk frå merknadene frå EFN.

*TONO* ser på framlegget om å kriminalisere spreiking sjølv når dette skjer utan økonomisk motiv, som «en styrke ved lovforslaget, da det etter hvert vil bli vanskeligere å dra et fornuftig skille mellom privat og kommersiell virksomhet på nettet, men hvor skaden kan være akkurat den samme for rettighetshaverne. Dette henger bla. sammen med at inntjeningsmulighetene for en eier av en hjemmeside kan relatere seg til helt andre ting enn det faktiske utbud av utstyr eller programvare. Det behøver nemlig ikke å ligge et vinningselement i selve utbudet, eller omvendt at nettstedet kan ha banner/sponsor/reklameinntekter selv om det er en privat hjemmeside til en fingernem student.»

Også *Antipiratgruppa* ser framlegget om utviding som ei klar forbetring. Gruppa peiker på at omgrepet «spredning til en videre krets» må få ei nærare avklaring.

*Nærings- og handelsdepartementet* «er positive til at lovforslaget, i likhet med det danske forslaget, kriminaliserer ikke-kommersiell utbredelse av ulovlig dekodingsutstyr til en videre krets».

Det er noko større sprik mellom høyringsinstansane når det gjeld kva for reint private aktivitetar som bør vere straffbare. Både *Antipiratgruppa* og *TONO* vil kriminalisere også privat innehaving, slik som i Danmark.

*EFN* på si side understrekar at det ikkje er sjølv koden som er verna av § 262, men derimot «rettighetene og vederlaget til åndsverket som formidles. Det er vitalt at tilegnelse, besittelse og formidling av kunnskap om dekodings- og krypteringsmetoder i seg selv ikke kriminaliseres».

Spørsmålet om straff for å inneha dekodarinnretningar må etter departementet sitt syn sjåast i samanheng med spørsmålet om straff for knekking av kodar.

*TONO* uttaler om dette at det er nødvendig å «se på muligheten av en fremtidig strengere regulering av selve det å «hacke» krypteringskoder, uansett om dette er for å skaffe seg en rettsstridig vinning eller ei». Også *ØKO-KRIM* meiner dette spørsmålet ikkje kan løysast i denne omgang fordi det «reiser mange vanskelige problemer».

*EFN* uttaler at ein «ser det som overordnet viktig at man ved denne lovendringen ikke kriminaliserer noen som bryter en sperring i den hensikt å få oppfylt rettigheter som han har krav på etter åndsverkloven».

*Departementet* meiner, som tidlegare, at det vil vere å strekkje forbodet for langt, om ein kriminaliserer det å inneha dekodarinnretningar. Då kan ein risikere å kriminalisere innehaving av innretningar som har både legale og illegale bruksområde. Ut frå omsynet til effektiv bevisføring ville det sjølv sagt vore ein fordel om innehaving var nok til straff. Då ville det t.d. ikkje vere behov for nærare undersøkingar av om innretninga hadde vore i bruk. I denne vurderinga kan ein likevel ikkje berre sjå på behovet for å sikre vederlag til dei verna tenestene. Ein må óg ha klart for seg dei omsyn som talar mot kriminalisering av det å inneha.

Interessa for datateknologi er stor, og mange viktige innovasjonar har kome som eit resultat av at private, «uautoriserte» personar har utforska det utstyret og den programvaren dei har fått i handa. Mellom anna av omsyn til den framtidige utviklinga av datateknologien, samt retten til omvendt utvikling i åndsverklova §§ 39 h og 39 i, er det ikkje aktuelt å foreslå kriminalisering av kodeknekking og det å inneha kodarinnretningar.

## 6.7 Strafferamme

---

I høyringsbrevet vart det gjort framlegg om ei strafferamme med bøter eller fengsel inntil 1 år for brot mot reglane i første og andre ledd (i denne proposisjonen er dette no samla i første ledd) og berre bøtestraff for ulovleg bruk av piratinnretningar.

Ingen av høyringsinstansane har kommentert dette. Departementet har likevel kome til at strafferamma for ulovleg bruk bør endrast til bøter eller fengsel inntil 6 månader. Det er to grunnar til dette. For det første er det ikkje grunnlag for å nedkriminalisere privat bruk så kraftig. I dag er strafferamma inntil 1 års fengsel. For det andre blir det dårleg samsvar mellom § 262 og strl.

§ 391 a fjerde ledd om det ikkje lenger skal vere fengselsstraff for ulovleg bruk. Når fengsel kan nyttast for brot på § 391 a - som er rekna som misferd - må ein ha minst same strafferamme for alle alternative brot på § 262 - som er rekna som brotsverk. Likevel vil det vel ikkje vere særleg aktuelt - når strafferammene blir dei same - å nedsubsumere eit brot på § 262 til eit brot på § 391 a fjerde ledd. § 391 a fjerde ledd kan derimot vere eit aktuelt alternativ for brot mot § 262 første ledd, når «straffeskylden må regnes for liten» av dei grunnar som er nemnde i § 391 a første ledd.

## **7 Økonomiske og administrative konsekvensar**

Framlegget i denne proposisjonen vil ha svært avgrensa økonomiske og administrative konsekvensar. Det kan bli nokre fleire saker for påtalemakta fordi også informasjonssamfunnstenester blir omfatta, og dermed nokre fleire straffesaker for domstolane. På den andre sida medfører framlegget ei opprydding i føreseigna som kan gjere arbeidet for påtalemakta enklare.

Departementet reknar med at føreseigna i første rekkje vil ha ein allmennpreventiv effekt, ved at potensielle profesjonelle distributørar av piratinnretningar avstår frå slike aktivitetar som vert råka av lovforbodet. Føreseigna vil vere grunnlag for private erstatningssøksmål frå leverandørar av verna tenester mot personar og selskap som krenker deira vederlagsinteresse. Dette kan gi nokre fleire sivilrettslege saker for domstolane.

## 8 Merknader til føreseгна

### 8.1 Innleiing

---

Framlegget til endringar i straffeloven § 262 kan kritiserast for å vere noko tungt oppbygd. Føreseгна har fått to ledd (tredje og fjerde) som berre inneheld definisjonar av omgrep som vert nytta. Departementet kan likevel ikkje sjå at dette kan gjerast på andre måtar om ein skal få til den nødvendige presisjon.

### 8.2 Første ledd

---

Første ledd omfattar aktivitetar som kan ha som resultat at dekodarinnretningar blir tilgjengelege for brukarane utan autorisasjon. Bokstav a og b rår aktivitetar som vert utført med vinning som målsetting («vinnings hensikt»), medan bokstav c rår den som utan vinning som målsetting søker å spreie slike innretningar.

Aktivitetane rekna opp i bokstav a er identiske med verksemdene rekna opp i direktivet artikkel 4 bokstav a og b. At også innehaving («besittelse») av dekodarinnretningar er gjort straffbart, når føremålet med innehavinga er vinning gjennom å skaffe nokon uautorisert tilgang til verna tenester, får til følge at påtalemakta kan reise sak sjølv om ein ikkje har bevis for at innehavaren har gitt frå seg dekodarinnretningar til andre. Det er nok å føre bevis for at føremålet med å ha innretningane har vore seinare overlevering (sal, utleige, utskifting mm.) til piratbrukarar mot vederlag.

Omgrepet «distribuerer» femner vidt, både etter ordlyd og intensjon, og har her same tyding som i fortalen til direktivet, punkt 20. I den norske omsetjinga heiter det her at distribusjon «omfattar alle former for formidling i tillegg til marknadsføring av slike innretningar med tanke på omsetnad i eller utanfor Fellesskapet». Ser ein på den engelske teksta, er det noko som tyder på at omsetjinga ikkje er heilt treffande. I den engelske versjonen av direktivet heiter det at distribusjon «includes transfer by any means and putting such devices on the market». <sup>4)</sup> På norsk ville det vore ei betre omsetjing om ein hadde sagt «framby for sal» eller «leggje fram for sal» i staden for «marknadsføring». I norsk samanhang elles tyder «marknadsføring» i første rekkje annonsering og reklamering, noko som er direkte omtala i direktivet artikkel 4 c og lovframlegget § 262 første ledd b.

Ordlyden i bokstav b dekkjer direktivet artikkel 4 bokstav c, men det er her valt ein noko annan ordlyd fordi direktivteksta på dette punktet kan synast litt uklar. Ordlyden i lovframlegget ligg tett opptil ordlyden i den danske radio- og fjernsynsloven § 75 a andre punktum («Annonsering eller anden form for reklame for sådant utstyr er ikke tilladt»). Det følgjer allereie av vilkåret om

---

<sup>4)</sup> I den svenske versjonen har ein nytta omgrepet «saluföring» og i den tyske «Vermarktung».

«vinnings hensikt» at bokstav b ikkje råkar den som på eit reint ideologisk grunnlag gjer seg til talsmann for bruk av piratinnretningar. Om denne personen samstundes er innblanda i omsetning av slike innretningar, kan meir politisk prega utsegner etter tilhøva likevel bli råka. Spreiing av handbøker, oppskrifter og liknande om korleis ein skal gå fram for å skaffe seg piratinnretningar, fell derimot utanfor bokstav b. Spreiing av slik kunnskap kan etter tilhøva likevel bli råka av regelen om medverknad.

Forbodet i bokstav b rettar seg mot dei eller den som står bak annonsen og ikkje den som berre medierer annonsen (formidlar annonsen gjennom sitt medium). Om dei subjektive vilkåra er til stades, kan den ansvarlege for mediet som vert nytta etter tilhøva bli straffa etter reglane om medverknad.

Omgrepet «vinnings hensikt» i bokstav a og b er å forstå som i strafferetten elles, sjå mellom anna strl. § 257 og § 255. Det er ikkje - som i direktivet - noko krav om kommersiell verksemd, som kan leie tanken mot næringsverksemd eller i alle fall at dei ulovlege aktivitetane må ha eit visst profesjonelt preg. Etter framlegget er det nok med eit einaste tilfelle. Omfanget vil derimot vere av interesse ved utmåling av straff.

Etter bokstav c er det ikkje eit vilkår at den ansvarlege har ei målsetting om vinning. Dette alternativet vil derfor typisk råke den som spreier dekodarinnretningar i form av programvare via internett. Om det skjer fordi vedkommande vil gjere andre ei venneteneste eller av andre grunnar, er utan interesse. Omgrepet «søker å utbre» har her same innhald som i straffeloven § 204 første ledd a. Det inneber at gjerningsmannen må ha freista å gjere dekodingsinnretninga tilgjengeleg for ein større krets av personar, i motsetnad til ein person eller svært avgrensa krets. Korleis utstyr og programvare blir spreidd, har ingen interesse. Dette vil difor t.d. ramme spreieing via opne og lukka nyhetsgrupper, «chatlines» og «FTB-sights» på internett eller spreieing til ein større krets via SMS-meldingar. Som etter strl. § 204 første ledd a ligg det i «søker å» at det føreligg eit fullført brotsverk sjølv om spreieing faktisk ikkje har funne stad.

Av slutten på første ledd følgjer eit subjektivt vilkår som gjeld både bokstav a, b og c, og som difor for både a og b sitt vedkommande kjem i tillegg til det subjektive vilkåret om at gjerningspersonen må ha hatt vinning som føremål. For å vere i strid med loven må føremålet med aktivitetane i bokstav a til c vere «å skaffe noen uautorisert tilgang til en vernet tjeneste». Dette inneber at den som t.d. sel eller leiger ut dekodarinnretningar etter avtale med den som står bak den verna tenesta som innretninga gir tilgang til, ikkje er omfatta av forbodet. Føremålet med aktiviteten er jo då å gi *autorisert* tilgang til ei verna teneste. Utan dette subjektive kravet ville dei fleste former for spreieing av legale dekodarinnretningar bli råka. Her kan det nok dukke opp grensetilfelle der det er uklart om dekodarforhandlaren har nødvendig avtale med den - eller alle dei - verna tenestene som innretninga kan gi tilgang til. Gjerningspersonen har då berre handla i strid med § 262 første ledd om det kan provast at føremålet var å skaffe nokon uautorisert tilgang i tillegg til den autoriserte.

Det er naturleg å sjå det slik at vilkåret om at føremålet må vere å skaffe nokon uautorisert tilgang, er oppfylt sjølv om mottakaren/kunden ikkje veit at innretninga kan gi slik tilgang.

Større vanskar kan dette vilkåret skape i høve til dei som sel, leiger ut mm. innretningar som har eit klart legalt bruksområde, men der innretningane - slik dei er eller ved enkle endringar - også kan nyttast som piratinnetningar. Ukoda smartkort kan her vere eit eksempel. Fordi desse korta har legale bruksområde - som til dømes dørkort - kan ein ikkje innføre eit forbod mot omsetning av slike. Samstundes kan desse korta programmerast slik at dei kan gi uautorisert tilgang til t.d. koda fjernsynssendingar.

Ofte vil det ikkje vere vanskeleg å føre prov for at målsettinga med aktiviteten er å legge tilhøva til rette for at kundane kan få uautorisert tilgang til verna tenester. Det kan følgje direkte av annonseringa for innretningane, om den t.d. inneheld opplysningar om at innretningane har illegale bruksområde. Det kan óg følgje av at gjerningsmannen har sett saman ei pakke av innretningar som kvar for seg har legale bruksområde, men der den kombinasjonen som føreligg, ikkje kan ha noko anna fornuftig føremål enn uautorisert tilgang. Eller det kan følgje av at innretningane blir omsette saman med opplysningar om kor kunden kan skaffe seg tilgang til den programvara som er nødvendig for å aktivisere innretningane.

Derimot vil det - som eit utgangspunkt - neppe vere nok til domfelling at ein på reint statistisk grunnlag kan syne at hovudtyngda av dei innretningane som ein gjerningsmann har omsett, blir brukt som piratinnetningar. Ein kan t.d. tenkje seg at ein forhandlar av elektronikk for koding av smartkort forstår at ein god del av kundane neppe treng utstyret for legale bruksområde. Forhandlaren kan t.d. i løpet av eitt år ha omsett 1000 einingar, og sjølv lagt til grunn at minst halvparten har gått til illegalt bruk fordi det legale bruksområdet er avgrensa. Om dette skulle vere nok til domfelling, blir forhandlaren sett i ein svært vanskeleg situasjon. Han eller ho må då anten - på statistisk grunnlag - nekte å selja innretningane til vel halvparten av kundane, men dette vil ikkje hindre at om lag same prosent av innretningane fell i gale hender, eller han må vurdere den einskilde kunden med sikte på å avgjere kven som kan ha illegale motiv og ikkje. Det er ikkje rimeleg å settje forhandlarane i ein slik situasjon. Eit regelverk som slik oppmodar forhandlarar til diskriminering på tilfeldig grunnlag, kan dessutan vera urett av andre grunnar.

Om forhandlaren derimot på noko vis hjelper dei kundane som spør, med opplysningar om korleis innretningane kan nyttast med sikte på uautorisert tilgang, vil det vere naturleg å sjå det slik at det subjektive vilkåret i § 262 første ledd i.f. er oppfylt. Då vil det framstå som rimeleg klårt for forhandlaren at *føremålet* til kunden (mellom anna) er uautorisert tilgang, og då vil føremålet med heile transaksjonen - også sett frå forhandlaren si side - bli det same.

Også medverknad til brot på første ledd er straffbart. Det er ikkje nødvendig at den som medverkar til brot på bokstav a og b har vinning som målsetting. Det gjeld sjølvsagt også for bokstav c, der dette vilkåret heller ikkje er retta mot hovudmannen. Derimot er det eit vilkår for straff at den som har medverka, har hatt som målsetjing å skaffe nokon uautorisert tilgang til ei verna teneste. Reglane om medverknad vil etter tilhøva kunne råke den som knekker ein kode og overlet denne til ein ven eller andre, når han veit at koden t.d. vil bli lagt ut på ei internettside.

Strafferamma er den same som i gjeldande § 262.

### 8.3 Andre ledd

---

Reglane i andre ledd råkar bruken av illegale dekodarinnretningar. Vinning ligg m.a. føre når ein ved bruken har hatt ei innsparing, t.d. om ein har sett ein film som ein elles skulle ha betalt for. Det frittek ikkje for straff at gjerningspersonen ikkje ville ha sett filmen dersom han eller ho hadde måtte betale. Det er ikkje tatt inn i føreseigna at vinninga må vere urettmessig då dette følgjer direkte av omgrepet «uautorisert tilgang».

Skyldkravet etter andre ledd er forsett, og forsettet må omfatte det at ein veit at innretninga som vert nytta, gir uautorisert tilgang. Det inneber at t.d. ei barnevakt som ser «video-on-demand» ved hjelp av piratutstyr medan eigaren er borte, ikkje blir råka om barnevakta ikkje visste at tilgangen var uautorisert.

Ordlyden rammer berre den som *bruker* innretninga, dvs. den som utfører dei handlingane som skal til for at innretninga blir aktivisert og/eller teken i bruk i det enkelte tilfelle. Dette inneber at personar som berre er til stades, ikkje blir råka, sjølv om dei er med på «tjuvkiking» og sjølv om dei veit at tilgangen til den verna tenesta er uautorisert. Dette fylgjer også av at andre ledd ikkje har straff for medverknad.

At strafferamma er lågare i andre ledd enn etter første, reflekterer at bruk er eit mindre alvorleg lovbrót enn dei aktivitetane som er omhandla i første ledd, jf. dessutan kapittel 6.7.

### 8.4 Tredje ledd

---

Tredje ledd inneheld ein definisjon av dekodarinnretning. Det er meininga at definisjonen skal fange opp eitkvart hjelpemiddel som har den eigenskapen at det - åleine eller saman med andre hjelpemiddel - kan gi tilgang i forståeleg form til ei verna teneste. Dette vil typisk vere elektronisk utstyr (hardware) og programvare (software).

Slik definisjonen er utforma, råkar han alle innretningar utan omsyn til om dei kan nyttast eller blir nytta til lovlege eller ulovlege aktivitetar. Dette er nødvendig fordi det i enkelte tilfelle ikkje er mogleg å avgjere om omsetning, bruk osv. av den aktuelle innretninga er lovleg eller ulovleg før ein har klargjort kva som føreligg av avtaler mellom forhandlar, brukar osv. og tenesteytar og/eller hans representantar, jf. nærare om dette i kapittel 6.4.

### 8.5 Fjerde ledd

---

Definisjonen av verna teneste ligg tett opptil direktivet artikkel 2 (a). Omgrepet «fjernsyns- og radiosignal» i bokstav a dekkjer i røynda det same som «kringkasting» i lov 4. desember 1992 nr. 127 om kringkasting § 1 første ledd. Av mellom anna pedagogiske omsyn har ein her valt å nytte ordlyden i gjeldande § 262.

Omgrepet «teleformidles elektronisk» i bokstav b er tatt frå definisjonen av informasjonssamfunnstenester i artikkel 1 nr. 2 i direktiv 98/34/EF, slik dette lyder etter endringa ved direktiv 98/48/EF, sjå nærare om dette i kapittel 3.2.

*Teleformidling* vil seie at ei teneste vert ytt utan at partane er til stades samstundes, medan omgrepet *elektronisk* viser at tenesta blir sendt og motteken

ved hjelp av utstyr for elektronisk databehandling og datalagring. Om tenesta kjem via kabel, radiomagnetiske eller elektromagnetiske bølger er utan interesse for definisjonen.

Med «forespørsel fra den enkelte tjenestemottaker» siktar ein til at tenesta blir ytt ved overføring av data etter ei individuell bestilling frå mottakaren.

Tilgangskontroll kan riggast til på mange måtar, og nokre gonger vil sjølve tilgangskontrollen vere ei eiga teneste. Også slike tenester er verna, noko som kjem fram i fjerde ledd i.f.

## **8.6 Femte ledd**

---

Femte ledd første punktum er likt med gjeldande § 262 andre ledd. I andre punktum vert det presisert kven som kan reknast som fornærma etter føresegna.

Justis- og politidepartementet

t i l r å r :

At Dykkar Majestet godkjenner og skriv under eit framlagt forslag til proposisjon til Stortinget om lov om endring av straffeloven § 262 (rettsleg vern av koda tenester).

---

**Vi HARALD,** Noregs Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjere vedtak til lov om endring av straffeloven § 262 (rettsleg vern av koda tenester) i samsvar med eit vedlagt forslag.

## Forslag til lov om endring av straffeloven § 262 (rettsleg vern av koda tenester)

### I

Almindelig borgerlig Straffelov (straffeloven) 22. mai 1902 nr. 10 § 262 skal lyde:

*Den som*

- a) i vinnings hensikt framstiller, innfører, distribuerer, selger, leier ut, besitter, installerer, vedlikeholder eller skifter ut dekodingsinnretning,*
- b) i vinnings hensikt annonserer eller på annen måte reklamerer for dekodingsinnretning, eller*
- c) søker å utbre dekodingsinnretning*  
*når hensikten er å skaffe noen uautorisert tilgang til en vernet tjeneste, eller medvirker til dette, straffes med bøter eller fengsel inntil 1 år.*

*Den som ved bruk av dekodingsinnretning påfører den berettigede et tap eller skaffer seg selv eller andre en vinning ved å få uautorisert tilgang til en vernet tjeneste, straffes med bøter eller fengsel inntil 6 måneder.*

*Med dekodingsinnretning menes i denne paragraf ethvert hjelpemiddel, enten dette er teknisk utstyr eller programvare, som er utformet eller tilpasset, alene eller sammen med andre hjelpemidler, for å gi tilgang i forståelig form til en vernet tjeneste.*

*Med vernet tjeneste menes i denne paragraf*

- a) fjernsyns- og radiosignaler, og*
- b) tjenester som teleformidles elektronisk på forespørsel fra den enkelte tjenestemottaker,*  
*når tilgang i forståelig form er avhengig av tillatelse fra tjenesteyter og ytes mot betaling, eller selve tilgangskontrollen til tjenestene nevnt i a og b, når den må regnes som en egen tjeneste.*

*Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale. Som fornærmet regnes også den som yter tilgangskontroll når denne må regnes som en egen tjeneste.*

### II

Lova gjeld frå den tid Kongen fastset.

---