Lee A. Bygrave (red.)

YULEX 2001

Institutt for rettsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 82-7226-060-3

Utgitt i samarbeid med Unipub Forlag
Trykk: GCSM AS

Forord

Denne boken er den første av en ny serie med årlige utgivelser fra Institutt for rettsinformatikk som går under tittelen Yulex. Siktemålet med serien er å tilby et rettsinformatisk julebord med «litt av hvert» – fra det lettleste og lett fordøyelige til det tyngre og fotnotebelastede. Serien skal også vise noen av de temaer som har opptatt instituttets medarbeidere gjennom året.

God jul og fornøyelig lesing!

Lee A Bygrave

Innhold

Meta-informasjon og Internett: Frem med stigen!

JON BING

«Informasjon» er et ord som brukes og misbrukes. Det er en del av dagligspråket, men også en fagterm i flere disipliner. Innen informatikken defineres gjerne «informasjon» sammen med triaden «tegn», «data» og «informasjon». I denne betydningen er et «tegn» betegnelsen på et symbol, en gest, et signal eller noe annet som alene eller sammen med andre tegn kan brukes til å danne «data». Data er en samling eller struktur av tegn som når den formidles frem til en person som har den nødvendige bakgrunn for å tolke den, forvandles til «informasjon». Et eksempel på et tegn er bokstaven «C», som uten kontekst knapt betyr noe som helst. Men hvis tegnet føyes sammen med andre tegn – f eks i formen «WC» eller «©» – blir det data. Hvis disse data formidles til en person, og personen er kjent med den aktuelle formalismen, blir de til informasjon: Den første gruppen har ofte vært kjærkommen for mange av oss i en trengt situasjon, den andre gruppen vil nok tolkes forskjellig alt ettersom man tror det bare er et symbol for «copyright», eller har innsikt i den internasjonale traktaten som definerer symbolet og tillegger det rettslig virkning i de land som er tilsluttet traktaten. Dette siste illustrerer at «informasjon» i denne betydningen har et subjektivt aspekt.

Dette er ikke begynnelsen på noe forsøk på å diskutere begrepet «informasjon», bare en påpekning av at uttrykket «informasjonsteknologi» egentlig blir en selvmotsigelse når man legger til grunn den definisjon som informatikken – det fag som utvikler og former denne teknologien – vanligvis bruker. For teknologi behandler data, ikke informasjon, i så måte var den mer gammelmodige betegnelsen edb («elektronisk databehandling») mer nøktern. Det gjør det også lettere å se sammenhengen i den historiske utvikling. For siden første gang et menneske presset et kileformet trestykke mot våt leire eller satte en meisel mot stein for å forme den første hieroglyf, har vi arbeidet med og videreutviklet vår «informasjonsteknologi».

Det er mange viktige sprang i denne utviklingen, og dette lille innlegget skal ikke forsøke å gi noen skisse av den. Men ett spennende skritt ble tatt da Gutenberg midt på 1400-tallet tok i bruk trykketeknikken. På det tidspunkt fantes det i Europa 30 000 bøker. Da hans nye kunst hadde vært brukt i 50

år, fantes det 300 boktrykkerier, ikke i Europa, men i Venezia! Og antallet bøker hadde økt til 15 millioner.

Naturligvis vakte også denne utviklingen av informasjonsteknologien tanker og kommentarer. Mot slutten av 1700-tallet skriver Ludvig Holberg et knippe epistler, bl a «Om gode og dårlige virkninger av boktrykkerkunsten».[1]

> «Derimod kand indvendes, at den Lethed og Magelighed, som Trykken fører med sig, foraarsager adskillige Uleiligheder. Derved bebyrdes Verden med en uhyrlig Mængde af unyttige Skrifter, og studerende Folk opfylder deres Hierner med vidløftig Erudition, givende sig hverken Tiid eller Middel til at reflectere paa hvad de læse. Herunder seer man i vor Tiid ikke saadanne rare Genier, som i gamle Dage, da studerende Mænd heller skierpede deres Hoveder ved idelig Meditiation, end opfyldte dem med vitløftig Læsning og med andres Tanker og Meeninger; Thi, ligesom en kand opfylde sit Huus med saa mange Giester, at han selv ikke faaer Rum at vende sig, saa kand og en opfylde Hiernen med saa mange fremmede Meeninger, at han intet Rum haver til egne Tanker».

Hvis vi hadde kunnet ha ført Holberg frem til vår tid og plassert ham midt i en moderne bokhandel, tror jeg han ville brutt sammen i krampegråt. Han ville se at hans verste anelser var gått i oppfyllelse. Hylle på hylle med unyttige skrifter, interesserte kjøpere ivrig opptatt med å anskaffe bøker for å fylle hodene med andres tanker. Og ingen som syntes at det var problematisk, tvert imot gledet foreldre seg over at barna leste – det var til og med opprettet organisasjoner med det formål å få folk til å lese mer!

En av de store forskjellene på Holbergs og vår tid, er utviklingen av *meta-informasjon*, dvs informasjon om informasjon. Når vi ikke fortviler ved inngangen til bokhandelen, kommer det av vår tro – kanskje av og til litt naive tro – på at vi kan beherske dette tilbudet, at vi kan «finne frem». Og vi finner selvsagt ikke frem ved å begynne nærmest døren og så lese titler bokhandelen rundt. Vi går målbevisst bort til hyller merket f eks «science fiction», vi utnytter bakgrunnskunnskap om forfatter og forlag, vi finner – kort sagt – frem!

Tradisjonelt finnes det flere former for meta-informasjon. Man kan godt sondre mellom strategier som brukes for å finne frem i en «enhet» med samme forfatter eller annet opphav (typisk en bok), eller å finne frem i en «samling av enheter» med forskjellige forfattere og avvikende utforming enhetene imellom (typisk et bibliotek, en bokhandel eller lignende). I prinsippet er det knapt noen skarp grense mellom enheter og samlinger av enheter (tenk bare på et arkiv), men i praksis kan vi tillate oss å operere med den.

---

1 Ludvig Holberg, *Epistler.* Utvalg ved Kjell Heggelund. JW Cappelens forlag, Oslo 1981.

Boken

Det er enklest å bruke en bok som eksempel. Bøker er i og for seg en «oppfinnelse» basert på utviklingen av pergament i byen Pergamon – byens bibliotek truet Alexandrias i renommé og størrelse, derfor heter det seg at Egypt forbød utføring av papyrus til Pergamon, og resultatet ble et alternativ. Pergament tillater bl a at man skriver på begge sider av arket, og representerte derfor en mer kompakt lagringsform enn papyrusrullene. En langsom konverteringsprosess frem til omkring 400 e Kr førte til at ruller ble erstattet med bøker. Rullene var forsynt med merkelapper som hang ut fra de hyllene de ble lagret i. For bøker ble det etter hvert vanlig å trykke stikkordinformasjon på ryggen – i dag standardisert til forfatter, tittel og forlag. Dette gjør det mulig å gå langs en rekke bøker å lese titlene, en enkel form for meta-informasjon.

En bok er i prinsippet en eneste lang linje med tekst, brukket opp av hensyn til sidens bredde og lengde. Den har en ubønnhørlig sekvensiell form. Det innholdet som skal presenteres, har sjelden bare én mulig struktur, og sjelden er denne sekvensielle – det har de fleste forfattere erfaring fra mens de slåss med «disposisjonen», som jo er betegnelsen på det problem å ordne emner inn i en sekvensiell struktur.

Denne strukturen erklæres gjerne gjennom en innholdsfortegnelse, som blir en meta-representasjon av den sekvensielle strukturen. De fleste bøker har en innholdsfortegnelse (det finnes unntak, særlig for skjønnlitteratur, men også for annen litteratur – Lovsamlingen har f eks ingen innholdsfortegnelse). De fleste av oss er flinke til å bruke innholdsfortegnelser. For det er jo slik – man kan like det eller ikke – at få fagbøker leses fra perm til perm. I praksis brukes ikke den sekvensielle strukturen av leseren på samme måte som den er brukt av forfatteren. Leseren «slår opp», gjerne på grunnlag av innholdsfortegnelsen. Det betyr nok en utfordring, fordi forfatterens omhyggelige pedagogiske fremstilling blir brutt av leseren, som slik lett kan gå glipp av forklaringer og forbehold som leseren burde hatt in mente ved lesning av det avsnittet han eller hun finner frem til.

Innholdsfortegnelsen bygger vanligvis på meta-elementer i selve den løpende teksten, nemlig overskrifter. En sekvensiell tekst brytes gjerne opp i ulike hierarkiske nivåer – kapittel, hovedavsnitt, avsnitt osv – det finnes flere konvensjoner for slik inndeling. Hvert nivå markeres. Det er gjerne en dobbelt markering – for det første en enkel kode som angir elementets sekvensielle og hierarkiske plassering i strukturen (kap 1, pkt 1.1), og dernest en overskrift eller tittel, som tar sikte på å karakterisere innholdet i det aktuelle elementet. Disse overskriftene vil tradisjonelt være tilordnet av forfatter, og altså være en del av den tekst forfatteren har skrevet – men det finnes mange nok eksempler på at en redaktør bistår med oppdeling mv. Det er disse over-

skriftene som sorteres frem til innholdsfortegnelsen, som derfor bygger på autentiske (forfatterskapte) elementer.

Av og til føyes det til enda et meta-element til teksten, et sammendrag, en telegrafisk stikkordkaratkeristikk eller lignende. I Charles Darwins *Rejse om Jorden*[2] finner man f eks denne karakteristikk av tredje kapittel:

> «Monte Video. – Maldonado. – Udflugt til R. Polanco. – Lazo og Bolas. – Agerhøns. Mangel paa Træer. – Hjorte. – Capybara eller Flodsvinet. – Tucutuco. – Molothrus, gjøgelignende Færd. – Tyran-Fluesnapper. – Spotfugl. – Aadselsfalke. – Rør dannede af Lynild. – Et Hus ramt af Lynild.»

I dette tilfellet er denne karakteristikken autentisk, og sikkert formet av forfatteren for å skjerpe leserens appetitt på det nedenstående kapittel. Men ofte er slike sammendrag tilføyd av en tredjeperson, typisk en redaktør – dette er ikke uvanlig i vitenskapelige tidsskrift, domssamlinger mv. Hovedfunksjonen for sammendrag og lignende meta-elementer er ikke egentlig å «slå opp» i boken, men å vurdere om hvorvidt det beskrevne element er relevant eller har interesse for leseren. Forsøk viser da også at sammendrag er særlig velegnede til å kunne avgjøre at det beskrevne ikke er relevant, og de har derfor ofte en betydelig nytteverdi i arbeidet med å orientere seg i en bok.

Det finnes strategier for å bygge inn strukturer som er alternative til den sekvensielle. Slike strategier realiseres gjerne ved registre, ofte kalt «bak-i-boken» registre etter deres konvensjonelle plassering. Det finnes mange typer registre, to viktige hovedtyper er stikkordregistre og systematiske registre.

Stikkordregisteret bygger i sin enkleste form på en sidebeskrivelse, noen – ofte forfatteren, men like ofte en tredjeperson – leser boken og skriver ned ord som synes karakteristiske for det boken behandler, side for side. Ofte baserer man seg på innfallsmetoden, det velges ord som fremstår som særlig betegnende. Det hender at dette fører til valg av ord fra overskrifter eller sammendrag, i så fall blir ikke stikkordregisteret et særlig viktig supplement til innholdsfortegnelsen. Eller man kan basere seg på å velge ord fra en forhåndsdefinert liste (tesaurus) i ønsket om å oppnå høyere grad av konsistens. Det kan også være veiledninger om ord man alltid skal plukke med seg – personnavn, stedsnavn, omtalte organisasjoner osv. Dette siste – regler som bygger på faste kriterier – vil også gi relativt høy grad av konsistens. Ofte vil man plukke ut enkelte slike stikkord og plassere dem i et eget register, i en juridisk monografi vil man f eks finne doms- og lovregister hvor referanse til lover eller dommer er stikkordene.

---

2 På dansk ved Emil Chr Hansen og Alfred Jørgensen, Brødrene Salmonsen, København 1876, s 42.

De systematiske registrene bygger på en systematisering av det domene boken omhandler. Denne systematikken vil gjerne være utarbeidet på forhånd og uavhengig av boken, og også være felles for flere arbeider innen samme domene. Jo mer utbredt, og jo mer stabil en systematikk er for domenet, desto bedre vil leserne kjenne systematikken, og jo lettere vil de kunne orientere seg ved hjelp av dem.

Slike registre representerer ikke bare meta-strukturer, men også hyper-strukturer, dvs alternative måter å organisere det materialet som i boken er tvunget inn på den rette linjes geledd. Et stikkord vil gi henvisning til flere sider hvor innholdet karakteriseres av dette stikkordet, disse samles til et knippe omkring det angitte emnet.

En tredje måte å danne hyper-strukturer på, er de tradisjonelle fotnotene som inneholder henvisning til andre steder i boken som er beslektet med den teksten noten er knyttet til. Dette er ikke meta-informasjon – fotnotene gir ingen oversikt over helheten – men knytter altså forbindelser i form av pekere fra en side til en annen.

Strukturen kan enkelt oppsummeres i en figur:

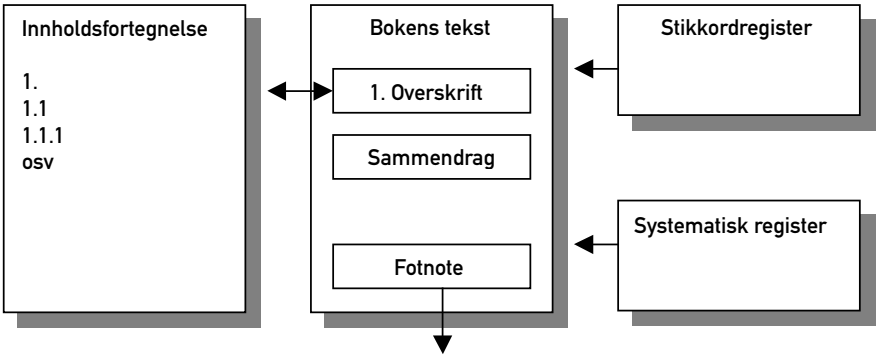


Fig 1: Meta- og hyper-strukturer i en bok

Når registrene etableres ved at en person – en indekserer – bruker egen forstand, kanskje hjulpet av regler, kalles dette intellektuell indeksering. Før datamaskinene hadde man egentlig ikke noe alternativ til dette, selv om det hendte – for særlig viktige forfattere eller verk – at man laget registre som

omfattet alle ordene i teksten, en tesaurus som ga henvisning til alle de steder hvor f eks Ibsen hadde brukt ett bestemt ord i sitt forfatterskap. Åpenbart krevde dette en stor og rutinepreget innsats, og investeringen kunne bare forsvares hvis hjelpemiddelet i neste omgang ville lette arbeidet med analyse eller tolkning av teksten.

Kanskje man til slutt kort bør reflektere over den rollen som sidenummer representerer. Sidenumrenes hovedfunksjon er ikke å opplyse om hvor lang boken er, men å gjøre det mulig å foreta entydige henvisninger innen boken. Det er på en måte en nokså grov referanse – finner man en henvisning fra personregistret til en bestemt side, må leseren selv lete gjennom siden for å finne hvor på siden navnet forekommer. Men selvsagt er sidenumrenes funksjon helt avgjørende nettopp for ved hjelp av meta-informasjon som registre å vise til hvor i boken noe forekommer. Det hender at man har alternativer til sideinformasjon qua nøkkel. I Lovsamlingen henvises det f eks ved hjelp av dato, ettersom lovene gjengis kronologisk, er dette like hensiktsmessig. Faktisk er det mer hensiktsmessig, for mens sidetallet vil kunne forandres fra utgave til utgave, vil datoen være stabil. Sidetallet er altså mediarelativt. Ved overgangen til digitale media, mister man sidetallet som referanse. Derfor utvikles alternativer, f eks en fortløpende nummerering av avsnitt, som vil være de samme i papir- og elektroniske utgaver.

Bibliotek

Et annet tradisjonelt eksempel er biblioteket, dvs en samling med mange enheter (i praksis bøker), gjerne skrevet av helt forskjellige forfattere. Hver av disse bøkene inneholder typisk den form for meta- eller hyper-informasjon som nevnt ovenfor. Men åpenbart vil dette gi liten hjelp til den bruker som vandrer inn mellom hyllene. Denne brukeren kan lese på ryggene av bøkene – og slik få en slags oversikt over hylleoppstillingen. Men det ville bli ørkesløse vandringer om man ikke hadde mer å hjelpe seg med.

Derfor har biblioteker egne registre i form av kataloger. Disse er igjen etablert etter ulike prinsipper, men tre vanlig forekommende typer svarer til de registre som kort er omtalt i forbindelse med en bok.

Utgangspunktet er gjerne et systematisk register, basert på en forhånd oppstilt systematikk. En klassisk systematikk kalles Dewey Decimal Classification System[3] etter Melvin Dewey, som utarbeidet den første versjonen av systemet i 1873, og publiserte det første gang i 1876. I dag inneholder det

3 Jf http://www.oclc.org/dewey/index.htm [15.4.2001].

110.000 ulike klassifikasjonsnøkler i et system som brukes av nasjonalbibliotekene i seksti land. Et enkelt eksempel på systemets hierarkiske oppbygning, som reflekteres i notasjonen, gjengis:

600	Technology (Applied sciences)			
	630	Agriculture and related technologies		
		636	Animal husbandry	
			636.7	Dogs
			636.8	Cats

Fig 2: Eksempel på Deweys klassifikasjon

I tillegg til systematisk katalog, vil man gjerne ha en forfatterkatalog. Denne er til liten hjelp for den som kommer til biblioteket med et problem uten forhåndskunnskap, men den vil ofte være til hjelp for den som kjenner sentrale forfattere mv. Det kan også være andre typer kataloger, f eks en emnekatolog som supplerer den systematiske katalogen – det hender man griper til det når en kategori får svært mange innførsler. I eksempelet kan man tenke seg at antallet bøker om katter i kategori 636.8 blir svært høyt. Da kan man enten utvide klassifikasjonen (6368.1 – «abyssinere»), eller supplere med en emneordkatalog innenfor den aktuelle kategorien.

Kanskje man bør understreke det arbeid som er nødvendig for å vedlikeholde kataloger. Dette gjelder ikke bare innføring av nye enheter som skaffes til samlingen, men også en stadig bearbeidelse av klassifikasjonssystemet slik at det utvides for å kunne reflektere ny viten og endret forståelse. Dette gjør slike systemer arbeidsintensive og kostbare.

Katalogene i biblioteket representerer meta-informasjon, og var kanskje de mest avanserte eksemplene før man fikk datamaskinbaserte systemer. Bibliotekets systematiske katalog var et kart over informasjonen som kunne tilbys fra hyllene. Likevel var det ikke enkelt å finne frem på egen hånd – derfor er biblioteker også bemannet med eksperter i utnyttelse av meta-ninformasjon, nemlig bibliotekarer. En bruker kan henvende seg til en bibliotekar, og selv om man mangler kjennskap til Deweys klassifisering eller andre hjelpemidler, vil bibliotekaren forstå henvendelsen han eller hun mottar i naturlig

språk, og på grunnlag av denne forståelsen selv utnytte tilgjengelige hjelpemidler for å finne forslag til hva brukeren trenger. Bibliotekarer er på en måte meta-informatikere, en profesjon man skulle ha trodd ville hatt en enda høyere profil i dagens virkelighet, hvor behovet for å finne frem i informasjonsressursene er aksentuert.

Det er gjort forsøk i å forbedre brukerens utnyttelse av bibliotekarer. Et par slike forsøk har hatt som hypotese at brukerens forespørsel er for knapp, og at man ved å forsterke interaksjon mellom bibliotekar og bruker skal kunne oppnå øket effektivitet. Paradoksalt nok fant man at den økede kontakten i stedet førte til redusert effektivitet (slik dette ble målt i disse eksemplene). Forklaringen kan være at bibliotekarer er flinkere til å formidle metainformasjon til brukere enn brukere er til å formidle spørsmål til bibliotekarene, og at interaksjonen på en måte forandrer brukerens forståelse av spørsmålet slik at det passer best mulig til katalogenes systematikk og begrensninger. Hvis dette er tilfelle, så har vi altså en illustrasjon av forholdet mellom meta-informasjon og informasjon, som viser hvordan det ene på ingen måte er upåvirket eller uavhengig av det andre.

Et bibliotek er ikke en isolert institusjon. Antagelig kommer flertallet av brukere til biblioteket med forespørsel om en bestemt bok – de vet allerede på forhånd hva de ønsker. Denne kunnskapen må komme et sted fra, og den kommer ofte fra andre bøker i form av henvisninger eller omtaler. Fagbøker innenfor et område etablerer gjennom henvisninger mv en nokså sterk hyperstruktur. En anbefalt måte å skaffe seg oversikt over et område, vil være å lese et standard innføringsverk – og så følge henvisningene fra dette til den litteraturen det refereres til. Det finnes egne systemer som nettopp tar sikte på å eksplifisere slike hyperstrukturer (navnene varierer mellom områder, men de omtales gjerne som «citation indexes»).

Ofte brukes nettopp forfatterregisteret når man får en forespørsel generert på grunnlag av en henvisning fra eksterne kilder. Det er nok ingen helt generell måte å henvise til en bok på, men forfatter og tittel inngår alltid i henvisningen. Og kommer en bruker til biblioteket med ønske om en bestemt bok, vil man ved hjelp av slike opplysninger kunne bestemme om boken finnes eller mangler på hyllene. (Eller kanskje den er lånt ut, noe som man forhåpentligvis finner svar på i utlånsregisteret.) Forfatterregister (med tilhørende elementer som tittel) har altså en funksjon som svarer til den sidenumrene har internt i en bok.

Skissemessig kan man derfor også oppsummere et bibliotek i en figur:

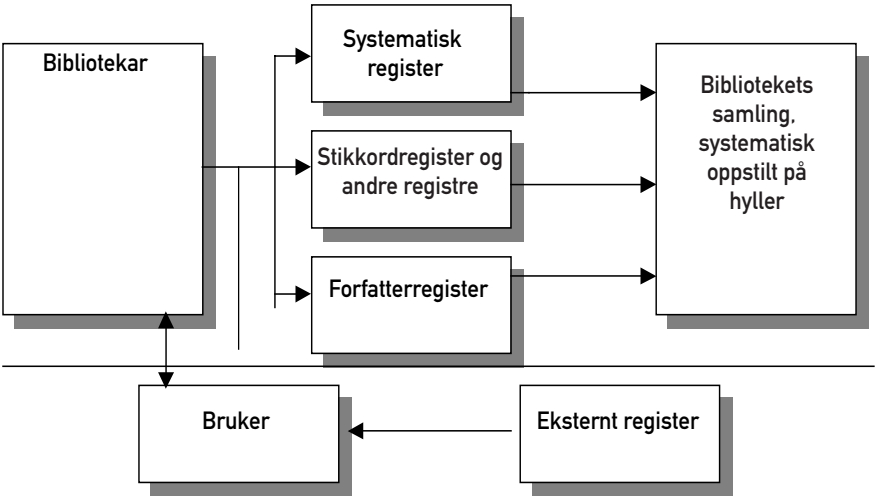


Fig 3: Informasjonssystemer rundt et bibliotek

Intellektuell og automatisk indeksering

Foran er det gitt flere eksempler på «intellektuell indeksering», dvs at en bok, artikkel eller annet dokument karakteriseres av en person på grunnlag av en klassifisering, tesaurus eller eget skjønn. Det er også nevnt at man unntaksvis også tidligere laget oversikter som inneholdt alle ordene i f eks en roman eller et viktig verk. Da man kunne bearbeid tekster ved hjelp av datamaskiner, ble det nokså trivielt å lage slike «inverterte filer», dvs registre som innehold alle forskjellige ord i ett eller flere dokument, med henvisning til hvor i dokumentet ordet forekom. I vanlige «bak-i-boken» registre var disse adressene begrenset til en sidehenvisning, i de datamaskingenererte registrene kunne adressen være svært nøyaktig: Dokument-, avsnitts-, setnings- og ordnummer. Ved hjelp av et slikt register, var det trivielt å be om å finne f eks en artikkel hvor ordet «Lille» forekom umiddelbart før ordet «Eyolf», og slik med stor sikkerhet finne artikler som omtalte Henrik Ibsens skuespill Lille Eyolf (1894) i motsetning til «Lille Herbern» eller «Eyolf Haug».

I begynnelsen sto det strid om effektiviteten av automatisk indeksering. Det ble med rette påpekt at datamaskinbaserte systemer ikke kunne utøve noe skjønn slik som en erfaren indekserer. Ordet «mark» ble oppfattet forskjellig fra ordet «eng», men beslektet med ordet «marg», datamaskinen la i utgangspunktet en rent syntaktisk behandling til grunn. Dette kan selvsagt

forbedres med bøyningsregler og unntak fra disse – en slik inkrementell forbedring kan skje nærmest uten begrensning. Men dette ville jo bety at man på en måte slo vrak på det som var den dramatiske fordelen med de datamaskinbaserte systemene: Nemlig at man ved marginale kostnader kunne etablere indekser over store volum av tekst. Tilhengerne av automatisk indeksering pekte på sin side på at man sjelden oppnådde konsistens ved intellektuell indeksering – ulike indekserere tilordnet de samme dokumentene ulike stikkord, faktisk ville den samme indeksereren tilordne det samme dokumentet ulike stikkord hvis det ble presentert for vedkommende på ny, sammen med andre dokumenter.

I dag er egenskapene ved intellektuell og automatisk indeksering vel kjent. Begge metoder har fordeler og ulemper. Men den altoverskyggende fordelen ved automatisk indeksering er at det gjør det mulig å lage søkesystemer uten prohibitiv kostnader i form av menneskelig innsats.

Det er faktisk litt kuriøst at det ble jurister – en profesjon som ikke nettopp er kjent som trendsettere i ny teknologi – som først tok disse mulighetene i bruk i stor skala. Det første tekstsøkesystemet for lover i autentisk form («full tekst») ble demonstrert i 1960, Norge fikk sitt første direktkoblede («on-line») rettslige informasjonssystem i 1981, og institusjonen Lovdata tilbyr i dag over 100 databaser med juridiske primærkilder.

Internettet og metainformasjon

Internettet bygger på et initiativ som ble tatt av det amerikanske forskningsdepartement i 1969, men er for lengst blitt et sivilt nettverk. Det er verdensomspennende, og kan i omfang bare sammenlignes med det større nettet for taletelefoni. Det har vært i bruk i Norge siden 1972 – faktisk var noden ved Kjeller utenfor Oslo den første utenfor USA.

Men Internettet forble et redskap for universiteter og forskningsinstitusjoner frem til begynnelsen av 1990-årene. Da ble det mulig for også andre å knytte seg til nettet. Og enda viktigere: I disse årene ble den tjenesten innen Internettet som heter World-Wide Web utviklet. Den første «nettleseren» ble tilgjengelig i mars 1993 – det var Marc Andressens Mosaic, tilbudt gratis til begjærlige brukere. Men ved utgangen av 1993 var det i hele verden bare omtrent femti datamaskiner knyttet til WWW. I løpet av de årene som er gått siden 1993, er – bokstavelig talt – Internettet blitt allemannseie, og Nettet er blitt en uunnværlig og dagligdags ressurs, ikke bare for forskere, men for alle som kommuniserer eller på annen måte arbeider med eller trenger informasjon.

Og mengden av informasjon er overveldende. Vi får sikkert lyst til å gjøre som Ludvig Holberg på terskelen til en moderne bokhandel: Sette oss ned og gispe litt av maktesløshet og frustrasjon. Hvordan skal vi orientere oss i

denne mengden av informasjon, hvor jo det aller, aller meste nettopp representerer «en uhyrlig Mængde af unyttige Skrifter»?

Foran er det brukt forholdsvis mye plass på å forklare meta-informatiske elementer i bøker og bibliotek. Grunnen er at dette fremdeles er de viktigste verktøyene vi har å hjelpe oss med i Internettets enda mer overveldende virkelighet.

En viktig form for meta-informasjon tilbys av søkemotorer. Disse fungerer i bunn og grunn på to måter, enten som intellektuell eller automatisk indeksering. Enkelte tjenester – som Yahoo! – har en omfattende klassifisering av nettsider. Det forutsetter intellektuell indeksering, selv om denne selvsagt er datamaskinassistert, indekserne benytter programmer som automatisk oppsøker nettadresser og leter etter ord eller fraser som kan indikere hva slags emne den aktuelle siden handler om, og så presentere dem til indeksereren for nærmere vurdering. Andre tjenester – som AltaVista – bygger først og fremst på automatisk indeksering: Systemet kopierer sider fra nettet som indekseres automatisk slik antydet ovenfor. Begge strategiene hjelpes av den underliggende strukturen for nettsidene. Sidene skrives ved hjelp av et sidebeskrivingsspråk, som godt kan oppfattes som en autentisk indeksering av siden. Hvis man f eks går til hjemmesiden for min egen institusjon (Institutt for rettsinformatikk, http://www.jus.uio.no/iri/), er dette en konvensjonell presentasjon av et institutt ved Universitetet i Oslo. Bak denne finner man en beskrivelse,[4] de første linjene i denne er:

```
<html>
<head>
<meta http-equiv=«content-type» content=«text/html;charset=iso-
8859-1»>
<meta name=«generator» content=«Adobe GoLive 4»>
<title>Velkommen til Institutt for rettsinformatikk</title>
<meta content=«Institutt for rettsinformatikk presenterer seg
selv, og tilbyr artikler, kommentert samling av lenker m.m.»>
<meta name=«keyword» content=«rettsinformatikk, data, juss, jus,
telekommunikasjon, personvern, opphavsrett»>
```

Ser man litt nedover, finner man et par linjer som definerer seg selv som «meta content» og «meta name». Hvis vi hadde ansvaret for en søkemotor, kunne det være nærliggende for oss å programmere den til å lete frem linjer med denne definisjonen, kopiere innholdet og legge dem til grunn for en auto-

4 Et eget valg i nettleseren viser «kilden» for de grafisk presenterte sidene.

matisk indeksering.[5] Dette bygger på den nærliggende hypotesen at her finner man nettopp ord som er karakteristiske for det innholdet som tilbys på dette nettstedet. Går man tilbake til den grafiske siden, vil man se at den har en tittel som svarer til den linjen som i utdraget ovenfor er definert som «title». Men de to linjene med «meta content» og «meta name» vises ikke – disse er lagt inn nettopp for å samvirke med slike mekanismer som søkemotorer og assistere i den automatiske indekseringen.

Karakteristisk for Nettet er også en sterkt utbygd hyper-struktur i form av lenker eller pekere. I prinsippet fungerer disse akkurat som henvisninger i fotnoter eller på annen måte innen en bok eller mellom bøker, slik som nevnt ovenfor. Men denne prinsipielle likheten med det tradisjonelle må selvsagt ikke få overskygge det nye, det som gjør hyper-strukturen kvalitativt forskjellig: Nemlig at man kan klikke på henvisningen, og dermed instruere programmet til automatisk å følge den henvisningen som er angitt i den underliggende representasjonen av siden, og slik «hoppe» til den siden det er henvist til.

Men det er for så vidt påfallende at vi ikke har fått helt nye former for meta-informasjon. Den frustrasjonen vi kan føle konfrontert med Nettets uoversiktlige tilbud kommer nettopp av at det er uoversiktlig, og at vi ennå ikke har gode nok hjelpemidler for meta-informasjon som skaper muligheter for effektiv gjenfinning og lett begripelig oversikt. Man vil finne nettsteder som har kart over det materialet som tilbys, av og til presentert som grafiske strukturer hvor man ser oppbygningen, og lett kan hoppe innen nettstedet – et slags motstykke til innholdsfortegnelser for materiale som ikke er ordnet sekvensielt. Men de fleste nettsteder er nok utformet som om de skulle være elektroniske bøker, til tross for at teknologien nettopp tillater flukt fra den lange, rette linjes tyranni.

Man må imidlertid ikke bli sittende igjen med det inntrykk at man innen den nye teknologien bare har parallellforskjøvet den typen registre mv som har hjulpet oss i en papirbasert verden, selv om dette i prinsippet ikke er så uriktig. Det finnes mange smarte muligheter som utnyttes. Til og med det enkle eksempelet som ble nevnt i forbifarten – «finn dokumenter hvor ordet 'Lille' forekommer umiddelbart foran ordet 'Eyolf'» – ville være vanskelig å realisere i den papirbundne verden: Selv om man hadde hatt et nøyaktig register med alle ordenes adresser, måtte man puslet sammen henvisningene for «Lille» og «Eyolf» på egen hånd for å finne i hvilke setninger de fulgte etter hverandre. Og det finnes mange strukturer i dokumenter som kan tolkes og utnyttes ved datamaskinbaserte metoder. Det finnes også mange spennende forsøk på å «forstå» naturlig språk ved hjelp av kunnskapsbaserte metoder

5 Derfor er også både formen «juss» og «jus» anvendt, slik at brukere vil finne siden uansett deres preferanse for staving av ordet.

(ofte omtalt litt misvisende som «artificial intelligence»), og spesielt innenfor begrensede domener er man kommet nokså langt – f eks ved produksjon av automatiske sammendrag.

Men vi har langt igjen. Trøsten får bli at det er en spennende vei å gå. Som et siste eksempel på hvor lang denne veien er, tilbyr jeg et forsøk gjort med et program som i markedsføringen reklamerer med at det kan oversette frem og tilbake mellom over tredve av verdens språk. I mitt lille useriøse forsøk valgte jeg den første strofen av fedrelandssangen: «Ja, vi elsker dette landet, som det stiger frem». Jeg valgte å oversette til «engelsk» (det var riktig nok et amerikansk flagg som indikerte valget, men pytt sann!). Og svaret kom: «Ja, we lover this country, as the ladder forward». Her gjenkjennes typiske eksempler på problemene ved maskinoversettelse: F eks at verb ble forvekslet med substantiver. Spesielt var jeg fascinert av frasen «Ladder forward!» Det har jo noe norsk over seg, ikke sant – kanskje en redingsdåd på åpent hav: Frem med stigen!

Og det er kanskje også et passende motto for den oppgaven vi står ovenfor i konstruksjonen av en bedre meta-informatisk oversikt over Internettet.

Building a legal framework for a virtual organisation in the maritime domain: the MARVIN experience[1]

EMILY M WEITZENBOECK

1 Introduction

The shipping industry, like other industries, has recognised the importance of information technology, not least the Internet, as a business and communications tool. A good information and communications infrastructure also enables and facilitates the formation of new forms of business co-operations such as virtual organisations. The EU-funded MARVIN project (EP29049), Maritime Virtual Enterprise Network, is developing software tools to support virtual enterprises in the ship repair and maintenance industry. A prototype software – the Maritime EnterpGriese, Jrise Integration Tool (hereinafter referred to as the "MEIT") – is being developed to model, facilitate and coordinate the interaction between maritime companies forming virtual organisations on the Internet, with the ultimate objective of minimising the docking time of ships to required repair and maintenance work.

One of the tasks during the MARVIN project was the development of a legal framework in the interest of both customers (ie, the shipowner or ship manager) and the partners who will supply services to them (eg, shipyards, salvage companies, classification society, etc) for the operation of a virtual maritime organisation. The focus of this task was the legal issues that arise from the creation and operation via the Internet of a virtual enterprise in the maritime domain. Other maritime law issues that may arise but which are not a consequence of the establishment of the virtual enterprise (such as the con-

---

1 This paper was originally prepared for the 7th International Conference on Concurrent Enterprising, Bremen, June 2001, and is reproduced in the proceedings of the conference: see Thoben, KD; Weber, F & Palwar, KS (eds), *Proceedings of the 7th International Conference on Concurrent Enterprising: 'Engineering the Knowledge Economy through Co-operation'* (Nottingham: Centre for Concurrent Enterprising, University of Nottingham, 2001), pp 337–345. The work from which the paper results, has been partly funded by the European Commission through ESPRIT Project *MARVIN: Maritime Virtual Enterprise Network* (No EP 29049). The author wishes to acknowledge the Commission for their support and the MARVIN project partners for their work in MARVIN. All errors remain those of the author.

sequences of oil pollution and damage, or of collision, or of injury or loss of life), were outside the scope of this task.

This paper starts with an analysis of the legal nature of the virtual organisation, with a look at the possible legal and business structures and contractual models that may be used for such organisations between the actors involved. This is followed by an analysis of the legal framework proposed in MARVIN.

2 The Marvin Virtual Enterprise

2.1 What is a Virtual Enterprise?

There are a number of different terms to describe the phenomenon of novel forms of economic organisations such as virtual organisation, strategic web, network organisation and strategic/co-operative alliances [Holland, 1998]. It is therefore important to clarify what is meant by the term "virtual organisation" or "virtual enterprise". Mertens & Faisst define the virtual enterprise [Odendahl, Angeli, 2000] as:

> "A virtual enterprise is a co-operation form of legally independent enterprises, institutions and/or individuals, that produce a service on the basis of a common business understanding. The co-operating units participate in the horizontal and/or the vertical collaboration with their core competencies and appear to third parties as a homogenous enterprise. Furthermore the institutionalisation of central management functions for design, management and development of the Virtual Enterprise are extensively abandoned and the necessary demand for co-ordination and harmonisation is covered by appropriate information and communication systems. The Virtual Enterprise is connected to a mission and ends with that mission."

Since a virtual enterprise is a co-operation form of legally independent enterprises, it may be formed among any of a number and mixture of the following business structures: sole traders, limited liability companies or other forms of partnerships or bodies of persons. In fact, the virtual enterprise offers small and medium-sized enterprises (SMEs) the advantage of collaborating together by pooling their resources and core competencies, so as to be able to offer a common service to the customer that each of them individually would not otherwise have had the resources to offer. This is a major advantage for SMEs.

There are a number of phases in the life-cycle of a virtual enterprise. Odendahl and Angeli [Odendahl, Angeli, 2000] list the following:

1. **Identification** of the need to co-operate, the definition of the goal to be reached by co-operation and the definition of the co-operation project is the initial phase.
2. **Partner Search:** This process is a selection of the partner companies out of a pool of potential offerors for the different core competencies needed in the Virtual Enterprise.
3. **Contracting:** Once the most suitable partners have been selected, the modalities of the co-operation should be determined through contracting between the partners.
4. **Operation:** This is the performance of the co-operation.
5. **Dissolution** of the Virtual Enterprise: This occurs once the task and goal of the Virtual Enterprise have been achieved.

2.2 The Virtual Enterprise in MARVIN

The second stage in the virtual enterprise life cycle could be performed by an external third party – a business integrator – that is trusted by all the potential virtual enterprise partners. Such a business integrator would typically have management, technological and engineering competencies. Odendahl and Angeli describe how the partner search task could also be automated by using the prototype system DEVICE of a co-operation exchange for Virtual Enterprises, which implements a five-layer filtering mechanism. Each layer constitutes a specific pre-set criterion (eg, price, competence, availability, etc) on the basis of which the potential offerors will be selected or "filtered". The mechanism to search for the most suitable partners used in the MEIT prototype is based on part of the prototype system DEVICE aforementioned [Odendahl, Angeli, 2000]. Web-based agents will support the partner search, the setting up and the operation of the virtual enterprise in the two business cases selected in MARVIN, that is, scheduled (routine) and unscheduled (emergency) repair.

In the MARVIN project, the MEIT will facilitate and co-ordinate the interaction and co-operation of companies building up a virtual organisation to carry out the repair of a ship in the shortest possible time. The MEIT is designed as a multi-agent system where every actor for each scenario, ie, both partner companies comprising the virtual enterprise (eg, shipyard (SY), emergency response company (EC), tug company (TC), classification society (CS), Salvage Company (SC)), as well as the customer (ie, ship manager (SM), shipowner (SO)), is represented by its own agent (cf Figure 1). An agent – an autonomous computational element which exists in the Internet and which contacts other elements of the Internet – represents the interests and goals of

the relevant participant of the virtual enterprise. Through the use of agent technology, the communication between the customer and the virtual enterprise will be partly automated. Every agent representing a special actor of the scenario operates as an expert system (having its own knowledge base of rules) with the goal to satisfy the needs of the enterprise it forms parts of and the customer respectively. [Odendahl et al, 2000].

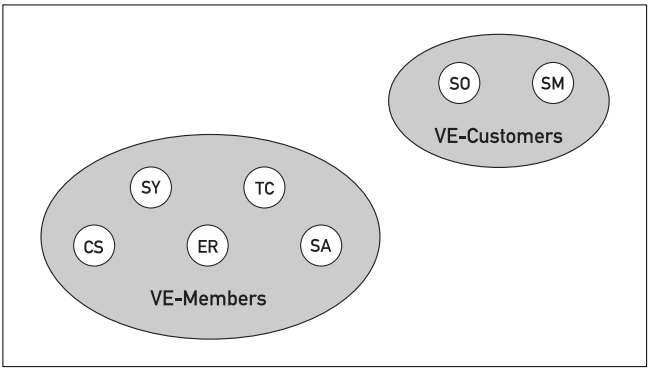


Fig 1: Some users of the MEIT

One could thus say that the MEIT, being a maritime enterprise integration tool, and, as its name implies, is performing many of the functions that the business integrator in a virtual enterprise performs. However, there will still be a role for a business integrator to act as a maritime services provider to administer the MEIT system and perhaps to offer added services to the users of the tool (ie, either potential virtual enterprise members or customers).

3 Business and legal structure of a Virtual Enterprise

Before proceeding to discuss the legal framework proposed for the virtual enterprise created via the MEIT, the question should first be raised as to what kind of business structure the virtual enterprise most resembles and whether it has a separate juridical personality.

In order to do this, one should first distinguish between two different types of virtual enterprise. On the one hand, there may a **stable** virtual enterprise where there is one core partner that lays down the rules for collaboration and that outsources certain tasks to other independent enterprises (eg,

Dell company, Amazon.com). This has also been referred to as top-down virtualisation [Odendahl, Angeli, 2000]. On the other hand, there may be **dynamic** networks consisting of individual independent enterprises which together embark on common action at the moment that a customer approaches them with an order or a problem. In the latter case, temporary collaboration results with shared leadership [Jansen, Steenbakkers, Jägers, 1999]. This has also been described as bottom-up virtualisation [Odendahl, Angeli, 2000].

3.1 Top-down Viritualness

In this model of a virtual enterprise – also called planet-satellite organisations – there is high control by the core partner, which outsources tasks to a number of legally independent units. One is likely to find that the core partner (planet) will enter into separate contracts with each of the smaller firms (satellites) to which it outsources tasks. Such contracts would lay down clear consequences (eg, through the imposition of heavy penalties or pre-liquidated damages) for non-compliance by the small firm, since such non-compliance (eg, delays in meeting deadlines, or refusal to perform) can have very serious consequences for the core partner. For example, a delay of one partner might mean that another enterprise would be unable to perform its part in the chain of production because of temporary unavailable resources or manpower. Such contractual clauses are one way for the core partner to try to limit the risks that ensue from its dependency on the smaller enterprises.

3.2 Bottom-up Virtual Enterprises

In this model of virtual enterprise, a number of economically and legally independent enterprises co-operate together to produce goods and/or services in a better way so as to be more competitive together in the market. Such co-operation forms may either be long-term oriented and based on the involvement of capital as well as contractual guarantees (these are sometimes also called strategic alliances or strategic networks) or else such co-operation forms may be short-term oriented, very flexible and dynamic (almost all definitions in literature on virtual enterprises refer to this latter form of organisation).

An important factor for business co-operation is trust. Trust plays an important role in both the strategic alliance and the virtual organisation. In strategic alliances trust is safeguarded through procedures and contracts. In dynamic virtual enterprises, according to some authors [Jägers, Jansen, Steenbakkers, 1998], in contrast with strategic alliances and planet-satellite organisations, "the virtual organisation participants do not try to heighten this control through regulation or forms of control (using contracts for example) but rather through the pooling of knowledge and information." However, it is submitted that although there might not be a pre-existing contractual relati-

onship between the independent enterprises forming a flexible and dynamic virtual enterprise (ie, pre-existing the partner search prior to the creation of a virtual enterprise), once the partners have been identified there will be a need to establish a legal framework for the virtual organisation. It might initially appear that a legal framework does not have to be considered because the concept of virtual enterprises is based on trust by definition. However, the application of such a culture of trust in practice has proved to be a problem, as this is opposed to the temporary character of a virtual enterprise because trust can only arise over a certain period of time (Odendahl, Scheer, 1999] (see also [Pletsch, 1998]). Therefore, virtual enterprises depend on loose legal frameworks, which may, for example, be implemented by electronic contracts.

3.3 Possible contractual formats

Three different legal contracting methods are conceivable [Berwanger, 1999]:

1. each firm contracts separately with the customer;
2. the customer contracts with one main partner which subcontracts to the other firms;
3. all individual members of the virtual enterprise jointly contract with the customer.

The first option has the consequence that each enterprise would only be responsible for its individual part of the performance and cannot be called to account for another's delays or non-performance. If the customer wants to raise a claim for breach of warranty (eg, defect) he would have to prove that a specific partner was responsible and sue only that partner. Furthermore, the customer is not assured that the whole product or service is performed completely, properly and on time. The risk of bad organisation and teamwork between the partner enterprises would be borne by the customer. Moreover, if the customer is contracting separately with each firm, an important feature of the virtual enterprise – that of providing one face to the customer – would be absent. This form therefore does not appear suitable for application to virtual enterprise contracts.

The second option – that one partner would have primary responsibility, contract directly with the client and then sub-contract to the other partner firms – would have the advantage for the customer that it can sue that one primary partner for any contractual breach or non-performance. Consequently, the risk borne by the primary partner would be great, as it would be acting as a main contractor. Small enterprises do not usually have the capacity to assume such risks and therefore this type of contractual structure is not very suited for virtual enterprises which is generally made up of SMEs.

This, however, is likely to be the typical contractual situation in a planet-satellite organisation.

The third option – where the individual partners in the virtual enterprise jointly contract with the customer – appears to be the contractual model most suited for a virtual enterprise. The contract would specify clearly the sharing of responsibility of all the service/product providers for the performance of the contract and the provision of the product or service to the customer. Each partner, in turn, could cover its liability by taking out appropriate insurance. The advantage for the customer is that he will not be dependent on just one partner and that partner's solvency for the performance of the contract.

The use of the word "enterprise" in the term "virtual enterprise" may be rather misleading to someone encountering this term for the first time, because it seems to give the impression that this is a new type of legal person. In fact, a virtual enterprise, though perhaps a new form of business co-operation, is not typically a separate juridical person. As abovementioned, one could use known and existing legal structures and mechanisms to regulate the operation of a virtual enterprise and the relationship between the members of the virtual enterprise and their customer. This can be through the use of a contract that resembles a consortium agreement to regulate the performance of the project, particularly in the case where all the individual members of the virtual enterprise jointly contract with the customer (as in alternative 3). Of course, in certain specific cases, the business partners may prefer to form a partnership (eg, a limited liability company), for example where a consortium's tender for a long- or medium-term project has been accepted and the business partners require a more formal and stabilised structure that can offer the benefits of limited liability.

4 A closer look at the MARVIN legal framework

4.1 Web-based contract for MARVIN

Any maritime business wishing to offer its services via the MEIT and wishing to be eligible for selection as a business partner in a future maritime virtual enterprise, would first have to register with the MEIT system. So would any potential customer of the virtual enterprise; ie, a shipowner or ship management company (cf Figure 1).

A variant of the third contractual model outlined above in section 3.3 in the form of an electronic contract was proposed for the maritime virtual enterprise created via the MEIT [Weitzenboeck, 2000]. This is because of some domain-specific peculiarities. In the MEIT, the partner search is limited

by some characteristics of the maritime domain. For instance, the classification society is pre-defined by the shipowner at the time when the ship is constructed (although the classification society may later be changed). Therefore there would already be a pre-existing contractual relation with a specific classification society. Similarly, the emergency-response company is usually predefined by the shipowner at the time the ship is acquired, because of the shipowner's obligation to comply with international maritime safety rules. Nevertheless, since the tool will be used to send information to and to receive information from both the classification society and the emergency-response company, such parties should agree on the validity of electronic communication through EDI contract-like clauses. This may be done by including such clauses in an online web agreement which all those who register with the MEIT (ie, potential service offerors and customers) should enter into before its registration in the MEIT system is accepted. It is proposed that such agreement – "the MEIT User Agreement" – should contain clauses on:

1. the use of the MEIT system by the users (i.e. those who register on the MEIT), and
2. the creation in future of a virtual enterprise by some of the users of the tool.

Some of the draft clauses for the MEIT User Agreement that were proposed in the MARVIN project are discussed in sections 4.2 to 4.6.

However, there are other partners with whom there will be no pre-existing contractual relationship (eg, a tug company or ship repair yard), and here the partner search and electronic contracting (phases 2 and 3 in the life-cycle of the virtual enterprise described in section 2.1) become relevant. Of course, such actors would also have to register and enter into the MEIT User Agreement like all the other users. Once such an actor, such as a shipyard, has been selected to carry out the repair the ship following an emergency or because of planned maintenance, there is a process of contract negotiation on the terms of the repair contract until agreement is reached and the repair contract is signed (see section 5 below).

An agreement such as the MEIT User Agreement is required to regulate the relationship between the users of the MEIT and the person maintaining the MEIT system (hereinafter referred to as the "Maritime Services Provider") as well as, to a certain degree, to lay down rules regarding the creation of a virtual enterprise in future by some of the users of the tool. Such an online contract would contain certain terms and conditions which one usually finds in agreements with an international character (since it is hoped that the parties thereto will be from various countries, both from within and outside

the EU), such as a choice of law clause, choice of forum clause, and a clause on liability.

4.2 EDI-related clauses

The extent to which a web-based contract such as the MEIT User Agreement is enforceable depends on the design of the actual contracting process. For example, a business wanting to register with the MEIT system should be required to first have scrolled through the contract terms screen before being allowed to proceed with registration on the system; it should have the option to leave the contract screen sequence at any point; and it should be required to indicate consent to the contract terms in an affirmative, unambiguous way which demonstrates its agreement to the displayed terms.

Moreover, the trend in Europe, following the E-Commerce Directive [E-Commerce Directive, 2000], is that contracts concluded by electronic means should not be deprived of legal effectiveness and validity on account of their having been made by electronic means. This Directive, in force since 17 July 2000, should be implemented by member states before 17 January 2002. Thus, it is to be expected that, at least within the 15 EU Member States, electronic contracts will not run the risk of being deemed invalid or without legal effect simply because they have been made by electronic means.

The situation may not be so clear as regards other jurisdictions. It is therefore recommended that a clause be inserted in the MEIT User Agreement whereby the users agree on the legal validity, effect and evidentiary value of the MEIT User Agreement and of any other contract effected through the MEIT with another user. This clause is loosely based on Article 3.1 of the European Model Electronic Data Interchange (EDI) Agreement [European Model EDI Agreement, 1994]. The difficulty that could arise with such a clause is that it could be considered to be a stipulation for the benefit of a third party (insofar as the MEIT User Agreement is a contract between the Maritime Service Provider and each individual user), and a number of legal systems do not always enforce such stipulations. What could be done to perhaps obviate this problem is to bind each user to include a clause, in its separate electronic agreements with other users of the MEIT, which upholds the legal validity of electronic contracts.

4.3 Compliance with the E-Commerce Directive

If the Maritime Services Provider is established inside the European Union, it should comply with the provisions of the E-Commerce Directive [E-Commerce Directive, 2000] since it would appear to fall within the scope of this Directive. The Directive applies to the provision of information society services which include services giving rise to on-line contracting, and include servi-

ces consisting of the transmission of information via a communication network, the provision of access to a communication network or the hosting of information provided by a recipient of the service (recital 18 in the preamble). This means that, for example, certain information such as the name and address of the services provider should be rendered easily, directly and permanently accessible to the recipients of the service and competent authorities.

4.4 Security and confidentiality

The need to ensure security of the MEIT system and confidentiality of the data transmitted via the MEIT is of paramount importance. This could be done through the use of passwords, through technologies that enhance security such as encryption & digital signature, and also through contractual obligations of confidentiality.

4.5 Choice of law & choice of forum

To obviate against doubts on the applicable law and forum to settle any potential disputes, an express choice of law and a jurisdiction clause should be included in the MEIT User Agreement. As to the question of which law should be chosen, a practical and appropriate choice is the law of the place where the Maritime Service Provider is established, or alternatively to choose a law and forum already commonly used in maritime trade (eg, London), as such a legal system would already be very familiar to the users of the tool.

4.6 Liability issues

Another issue that arises and becomes relevant once a commercial version of the MEIT has been developed and the system is available for commercial use, is what happens if the MEIT system malfunctions. Who would be liable: the programmer who programmed the system, the domain experts who provided the intelligence for the knowledge base of the system, the Maritime Service Provider, the MEIT users? In commercial contracts, it is common to try to limit liability up to the amount paid/earned on the contract by the party who suffered damages (eg, the contract price) through a cap on liability. One should also consider having a limitation on consequential, special, incidental and indirect damages to limit the Maritime Service Provider's exposure to open-ended liability.

5 Contracting among partners in the Virtual Enterprise & customers

As described in the life-cycle of the virtual enterprise in section 2.1, once the need for the creation of virtual enterprise has been identified (through the occurrence of an emergency or the need for maintenance), there is then a search for the partners with the required core competencies to come together to form the virtual enterprise. This is followed by contract negotiation and signature between the members of the virtual organisation and the customer.

However, as explained in section 4.1 above, in the field of emergency repair and planned maintenance, there are certain domain-specific peculiarities which limit the partner search, because a partner may already be pre-defined through pre-existing contractual agreements with the customer of the virtual enterprise. Therefore, naturally, there is no need for further contracts to be signed between such actors regarding these services.

Nevertheless, there are other partners with whom there will be no pre-existing contractual relationship (eg, the tug company or ship repair yard), and here the partner search and electronic contracting (phases 2 and 3 in the life-cycle of the virtual enterprise) become relevant. Once an actor, such as a shipyard, has been selected to carry out the repair the ship following an emergency or because of planned maintenance, there is a process of tendering, contract negotiation and agreement with regards to the repair contract.

A possible feature of the MEIT could be a facility, which allows the parties to select and agree on the terms and conditions, which are to govern such agreements (eg, towing and ship repair). Much of the contracting and sub-contracting in the maritime industry is done through the use of standard form agreements that have been developed by maritime associations such as Lloyds of London, especially in areas such as towing and salvage. Therefore, the contracting stage can be facilitated by the parties agreeing to use such standards contracts and incorporate them by reference.

6 Concluding remarks

A number of constraints were made on the design of the MEIT and the virtual enterprise created via the tool because of the peculiarities of the maritime domain. However, it is hoped that the experience and lessons learned in MARVIN will also be of interest and help in the design of a legal framework for virtual enterprises in other domains.

References

Berwanger, E: "The Legal Classification of Virtual Corporation According to German Law", in Sieber, P & Griese, J (eds), *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 1999* (Bern: Simowa Verlag, 1999), pp 157–159.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, pp 1 *et seq* ("E-Commerce Directive").

European Model Electronic Data Interchange (EDI) Agreement – Annex 1, 94/820/EC: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange. OJ L 338, 28.12.1994, pp 98 *et seq*.

Holland, CP: "The Importance of Trust and Business Relationships in the Formation of Virtual Organisations", in Sieber, P & Griese, J (eds), *Organizational Virtualness, Proceedings of the VoNet Workshop, April 1998* (Bern: Simowa Verlag, 1998), pp 53–64.

Jansen, W; Steenbakkers, W & Jägers, H: "Electronic Commerce and Virtual Organizations", in Sieber, P & Griese, J (eds), *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 1999* (Bern: Simowa Verlag, 1999), pp 53–66.

Jägers H; Jansen W & Steenbakkers W: "Characteristics of Virtual Organizations", in Sieber, P & Griese, J (eds), *Organizational Virtualness: Proceedings of the VoNet Workshop, April 1998* (Bern: Simowa Verlag, 1998), pp 65–76.

Odendahl, C & Angeli, R: "Final Virtual Organisation Architecture", MARVIN, Maritime Virtual Enterprise Network, ESPRIT project 29049, Deliverable T1.3D2, 2000.

Odendahl, C; Angeli, R; Haenisch, J; Jaramillo, D; Makris, S & Weitzenboeck, EM: "Web-based Virtual Enterprise Network for the Maritime Industry", in Stanford-Smith, B & Kidd, PT (eds), *E-Business: Key Issues, Applications and Technologies, Proceedings of eBusiness and eWork Conference, Madrid, October 2000* (Amsterdam: IOS Press, 2000), pp 559–565.

Odendahl, C & Scheer, A-W: "The Concept of Virtual Enterprises and its Relevance for the Maritime Domain", in Guedes Soares, C & Brooda, J

(eds), *Application of Information Technologies to the Maritime Industries* (Lisbon: Edições Salamandra, 1999), pp 11–31.

Pletsch, A: "Organizational Virtualness in Business and Legal Reality", in Sieber, P & Griese, J (eds), *Organizational Virtualness: Proceedings of the VoNet Workshop, April 1998* (Bern: Simowa Verlag, 1998), pp 85–92.

Weitzenboeck, EM: "Final Legal Framework for the Maritime Virtual Organisation", MARVIN, Maritime Virtual Enterprise Network, ESPRIT project 29049, Deliverable T1.4D2, 2000.

Opphavsrettslige utfordringer i informasjonssamfunnet

OLAV TORVUND

1 Utgangspunkt

Opphavsretten er et barn av informasjonsteknologi. Det var først da boktrykkerkunsten muliggjorde massespredning av litterære verk, at man begynte å føle behov for en rettslig beskyttelse av den type som etter hvert utviklet seg til opphavsrett.

Opphavsretten har alltid blitt utfordret av ny informasjonsteknologi. Viktige informasjonsteknologiske sprang, slik som cellulosepapir, rotasjonspresse, film, fjernsyn, båndopptagere, datamaskiner og internett, har alle satt opphavsretten under press. Men opphavsretten har utviklet seg gjennom disse utfordringene, og har til nå ov«erlevd. Jeg er også temmelig sikker på at opphavsrett i en eller annen form vil overleve også de utfordringer som dagens teknologi stiller den overfor, men den vil måtte tilpasse seg denne utviklingen. En grunn til en slik antagelse, er at vi trenger et rettslig regime som gir den som skaper et verk en form for vern. Ønsker vi at folk også i fremtiden skal ønske å gjøre resultatene av sin skapende innsats tilgjengelig for samfunnet, og dessuten at de faktisk skal ha muligheter til å bruke sin tid på dette, må man på en eller anen måte sikre at de kan høste fruktene av sin innsats.

2 Hvilken rett gir opphavsretten?

Opphavsretten gir en opphavsmann rett til å råde over sitt verk, ved å bestemme om det skal offentliggjøres eller utgis. Videre vil han kunne bestemme i hvilken form det eventuelt skal utgis, om det skal skje mot vederlag, osv. Man får ofte et inntrykk av at opphavsrett er det samme som at noen må betale for bruk av et verk. Men det er ikke alltid tilfellet. En opphavsmann kan ha mange grunner til å gjøre et verk tilgjengelig. Han kan håpe på at verket skal markedsføre ham og hans kompetanse, slik at han kan få inntekter på annen måte. Han kan brenne for saken, og ønske å spre sitt budskap til flest mulig uten tanke på betaling. Noen vil ha et ønske om å bidra gjennom å spre kunnskap, mens atter andre først og fremst nyter å se sitt eget

navn på trykk. Poenget er at det er opphavsmannen selv som kan bestemme om og i tilfelle hvordan hans eller hennes verk skal gjøres tilgjengelig.

Opphavsrett er en juridisk konstruksjon. Retten har ikke noe naturlig grunnlag, slik som eiendomsrett og vern av person. Man kan ikke verne om sin roman og hindre at andre utnytter den, slik man kan verne om sin eiendom. Opphavsmannen har de rettigheter i forhold til sitt verk som samfunnet har gitt ham gjennom lovgivningen, ikke noe annet.

Opphavsmannen har en enerett til å fremstille eksemplar av sitt verk. Utgangspunktet er at ingen kan kopiere denne artikkelen uten opphavsmannens samtykke. Videre har opphavsmannen enerett til å gjøre et verk tilgjengelig utenfor det private område. Et teater kan ikke sette opp et teaterstykke uten opphavsmannens samtykke, akkurat som man ikke kan stille ut en kunstners bilder offentlig uten at denne har samtykket til dette.

I tillegg har opphavsmannen visse ideelle rettigheter. Dette omfatter bl a retten til navngivelse. Men disse rettighetene vil ikke bli nærmere behandlet i det følgende.

Det er mange unntak fra disse rettighetene. Retten til privat kopiering – som ikke omfatter dataprogrammer – er allerede nevnt. Men det finnes flere. I denne sammenhengen vil jeg ikke gå nærmere inn på disse.

Utnyttelse av et verk som ikke innebærer eksemplarfremstilling, og som heller ikke innebærer at et verk gjøres tilgjengelig utenfor det private området, faller utenfor opphavsmannens enerett. Utgangspunktet er som nevnt at man ikke kan kopiere denne artikkelen uten opphavsmannens samtykke. Men man kan lese den så mange ganger man måtte orke. Og det er heller ikke noe i veien for at flere leser artikkelen, så lenge alle leser samme eksemplar. Man kan sende et tidsskrift på sirkulasjon, men man kan ikke kopiere opp de artiklene man anser som interessante og distribuere disse i en organisasjon.

I dag kan man se at rettighetshavere ønsker å begrense utnyttelsesformer som ikke innebærer eksemplarfremstilling eller tilgjengeliggjøring for allmennheten. Det er lett å tenke seg at man får rett til å spille musikken fem ganger før musikkfilen låser seg eller kanskje sletter seg selv, man kan ha rett til å se en video i 24 timer, osv. Men her gir ikke dagens opphavsrett noen løsning.

3 Utviklingstendenser som påvirker opphavsretten

Det kan ta meget lang tid å utvikle et åndsverk. En forfatter bruker lang tid på en roman, og det kan ligge mange årsverk bak utviklingen av en film eller et dataprogram. Men når verket først er skapt, er det ganske enkelt å reprodusere dette. Teknologien har gjort det noe enklere å utvikle verkene. Men først og fremst har den gjort det lettere å reprodusere dem.

Går vi tilbake til pre-Gutenbergsk tid, var det tidkrevende og dyrt å produsere en kopi av en bok. Bøker ble skrevet av ved at én leset høyt, mens en rekke andre – stort sett munker – skrev ned den tekst som ble lest opp. Det var den gang man hadde forelesninger i ordets egentlige betydning. Kopiering representerte den gang ikke noen trussel mot opphavsmannens interesser. Skulle man kopiere en annens bilde, måtte man male eller tegne et tilsvarende bilde selv. Reproduksjon av musikk, i alle fall fremføringer av musikk, var det neppe noen som kunne forestille seg muligheten av.

Vi skal ikke mange årene tilbake for å komme til en tid da kopiering ikke representerte noe stort problem. Det kostet så mye å lage lyskopier at man stort sett foretrakk å la et avskrivingsbyrå skrive av tekster. Går man til forarbeidene til den någjeldende åndsverksloven, ser man at kopiering til privat bruk eksemplifiseres med at noen skriver av et dikt som inkluderes i et kjærlighetsbrev til dennes elskede. Man fremstiller uten tvil et eksemplar av diktet, men slik eksemplarfremstilling representerer ikke noen trussel mot opphavsmannens interesser.

Dersom et verk foreligger i digitalisert form, vil alt være omgjort til binære tegn i form av et-tall og nuller. En CD plate med musikk inneholder ca 5 mrd slike tegn. En tekst representeres ved at hver bokstav tilordnes et tall. Man har også tall for de tegn som brukes, formateringsinformasjon, osv. En skriver eller et program som presenterer teksten på skjerm, tolker denne informasjonen etter de tolkingsreglene som er bygget inn i programmet. Et bilde representeres ved et koordinatsystem hvor hvert punkt har en numerisk adresse, og hvor hvert punkt har verdier for lysintensitet og farge. Film er bare serier av slike bilder. Lyd «samples» ved at man registrerer lydbildet flere tusen ganger i sekundet. All slik informasjon kan lagres på de samme medier, og overføres i de samme nettene.

Hvis verket er digitalisert, vil selv meget store verk kunne kopieres i løpet av kort tid, og til en meget lav pris. Og kopien er identisk med originalen. Man kopierer den binære koden som representerer f eks en musikkinnspilling, og kopien blir dermed identisk med og nøyaktig like god som originalen. Man opplever ikke lenger det som kalles et «generasjonstap» ved kopieringen, f eks at lydkvaliteten blir noen dårligere for hver kopiering. Enhver datamaskin er også en perfekt kopimaskin. Det lille hull i opphavsmannens vern som f eks kopiering til privat bruk representerte, har blitt større og større etter hvert som teknologien har gjort det enklere å foreta kopieringen.

Når et verk foreligger i digitalisert form, kan det også meget enkelt overføres. Man kan nå overføre tegnene i form av signaler som formidles via telenettet, og trenger ikke flytte noen fysiske objekter. Dermed blir det mulig å overføre et verk til den andre siden av jorden i løpet av noen sekunder. Og man kan lett spre det til svært mange på en gang.

Et tradisjonelt eksemplar vil i praksis bare kunne utnyttes av en eller noen få om gangen. Det er ikke lett for andre å lese mitt eksemplar av en bok så lenge jeg også leser i det. Så hvis det er en bok som mange ønsker eller har behov for samtidig, vil man anskaffe flere eksemplarer. Dermed får opphavsmannen i praksis en godtgjørelse for økt bruk, selv om opphavsretten ikke regulerer bruken i seg selv. Hvis verket er lagret i digital form på en tjenermaskin, vil mange kunne benytte det samme eksemplaret samtidig. Dermed vil ikke økt bruk nødvendigvis føre til at man anskaffer flere eksemplarer, og dermed vil heller ikke økt bruk automatisk føre til økt vederlag for den som har rettighetene til verket.

Et annet utviklingstrekk er at opphavsrettslig vernede verk, og dermed opphavsretten i seg selv, har fått en mye større økonomisk betydning. De største selskapene i verden er nå medieselskaper, og opphavsretten er fundamentet for deres virksomhet. Med større økonomiske interesser kommer også et større politisk trykk. Dette er ikke bare av det gode. Rettighetshaverne er godt organisert, og har vist seg som meget gode lobbyister. Brukerne kommer ikke like lett til orde. Opphavsretten forutsetter en balanse mellom opphavsmenns interesser i vern på den ene siden, og samfunnets interesse i kunnskaps- og kulturutvikling på den annen.

Det er lett å skyve forfattere og musikere foran seg, og gi inntrykk av at det er deres interesser man sloss for. Men ofte er det nok produsenter og distributører, og ikke de egentlige opphavsmenn som stikker av med den største gevinsten. De økonomiske interessene kan også bli en slags «gjøkunge» i opphavsretten, slik at de samfunnsmessige og kulturelle interessene som også skal ivaretas, skyves ut. Resultatet blir lett at balansen forskyves i opphavsmennenes favør, hvilket ikke nødvendigvis er til fordel for samfunnet som helhet.

Opphavsmannens dilemma er at han gjerne ønsker et så omfattende vern for sitt verk som mulig, samtidig som han vil stå mest mulig fritt til å utnytte andres verk. Jeg vil gjerne kunne bruke mest mulig av det som andre har skrevet om opphavsrett som grunnlag for denne artikkelen, men ønsker ikke at andre skal kunne utnytte det jeg har skrevet uten at jeg får vederlag. (Det siste er nok ikke helt sant. Men jeg kan late som om det er min holdning, for å få fram poenget.)

Et eksempel fra programvareindustrien kan illustrere dette. For noen år tilbake gikk Apple til sak mot Microsoft, med påstand om at visse elementer i Windows operativsystemet krenket Apples rettigheter til det grafiske brukergrensesnittet de hadde utviklet. Problemet var at Apple slett ikke har utviklet det grunnleggende selv. Man bygget på det som var utviklet av Xerox, ved deres forskningssenter Xerox PARC. På amerikansk vis ble selvsagt Apple saksøkt av Xerox, mens Apple fortsatt var i konflikt med Microsoft. Dermed befant Apple seg i den situasjon at jo mer overbevisende de argumenterte for

at de omstridte elementer var opphavsrettslig vernet slik at Microsoft hadde krenket deres rettigheter, desto mer styrket de argumentasjonen av Xerox i forhold til Apple. Og jo mer overbevisende de kunne argumentere for at det som var utviklet hos Xerox ikke var opphavsrettslig vernet, jo mer svekket de sin sak i forhold til Microsoft. Det hører med til historien at sakene endte med forlik, slik at de ikke ga noen avklaring av de rettslige spørsmålene.

Vi ønsker at opphavsmenn skal få incitamenter til å gjøre resultatene av sin skapende innsats tilgjengelig for samfunnet. Samtidig ønsker vi ikke at vernet skal bli så omfattende at det blir en bremsekloss i den kulturelle og kunnskapsmessige utviklingen. Det kan være mange meninger om hvor balansepunktet bør ligge. Men det er neppe særlig mye uenighet om at begge hensyn er viktige.

4 Distribusjon av informasjon og administrasjon av rettigheter

Den eldste form for informasjonsspredning er nok formidling fra en person til en annen. Det kan være foreldre som lærer opp sine barn, eller det kan være jegere som deler sin kunnskap om hvordan man kan finne byttet. Denne distribusjonsformen kan man kalle *konsulentmodellen*. Formen er ofte lønnsom for den som formidler informasjonen – i alle fall hvis informasjonen har noen verdi for andre. Man kan ta seg godt betalt for å gi denne informasjonen mer eller mindre eksklusivt til en annen. Ulempen er at informasjonen bare blir tilgjengelig for noen få.

Den neste modellen er *fremføring for en begrenset forsamling*. Dette kan være stammen som er samlet rundt leirbålet, publikum på et teater eller deltakerne på et seminar. Distribusjonsformen forutsetter at alle er til stede samme sted og til samme tid, Man kan kontrollere tilgangen ved å kontrollere adgangen til den arena hvor informasjonen presenteres, og man kan eventuelt ta betaling fra de som ønsker å komme inn. Dette gir nærmest en form for «bompengefinansiering» av informasjonen.

Man kan ha en variant av denne distribusjonsformen i elektroniske nett, ved ulike *abonnementsordninger.* Man vil ikke da begrense adgangen til det fysiske rommet, men i stedet kontrollere adgangen til den basen som informasjonen hentes fra. Her vil det ikke lenger være en forutsetning at alle er til stede samtidig, eller befinner seg på samme sted.

Ved *kringkasting* vil man i praksis ikke kunne kontrollere hvem som har tilgang til det som sendes ut. Men det vil være relativt få utsendelsespunkter, slik at man kan kontrollere utsendelsen. TONO kan f eks ta betalt fra alle

radiostasjonene, og behøver ikke tenke så mye på hvem som faktisk lytter til musikken (selv om dette vil kunne ha betydning for vederlagets størrelse).

Den tradisjonelle form for massespredning, er *spredning av fysiske eksemplarer* i form av kopier. Man vil da kunne administrere rettighetene ved å kontrollere produksjon og spredning av eksemplarer. Opphavsmannen vil da få et vederlag for hvert eksemplar som produseres og/eller distribueres. En forutsetning for en slik kontrollmodell er at man har få produksjonssteder for det enkelte verk. Jo flere produksjonspunkter, f eks i form av produksjon på forespørsel hos detaljister, desto vanskeligere blir det å kontrollere spredningen i denne modellen.

Ved spredning i nett bryter de tradisjonelle kontrollmodellene sammen. Det er en mange-til-mange distribusjon, som i praksis gjør det svært vanskelig å kontrollere så vel utsendelse som mottak. Napster-tjenesten har med all mulig tydelighet vist oss dette. Dette stiller oss derfor overfor nye utfordringer.

5 Teknisk beskyttelse

Moderne teknologi gir muligheter for mange nye beskyttelsesmekanismer. «Elektroniske bøker» er f eks ofte kodet slik at de bare kan leses på ett bestemt leseapparat. Filene kan kopieres, men andre vil ikke kunne lese dem uten at de samtidig låner mitt leseapparat. Og så lenge leseapparatet er utlånt til andre, vil jeg ikke kunne lese tekstene selv.

Den som har anskaffet programmer via internett er vel kjent med ulike begrensningsformer som kan benyttes. Det er vanlig at «shareware» distribueres slik at alle som ønsker fritt kan kopiere programmet til sin egen maskin. Men den versjonen som man installerer på denne måten vil være begrenset slik at man f eks bare kan bruke den i 30 dager. Hvis man ønsker å ha tilgang ut over denne prøveperioden, må man betale. Da vil man få tilsendt en «nøkkel» i form av en kode, som så «låser opp» programmet. En annen vanlig variant er at programmet bare kan brukes et antall ganger. Dessuten kan det hende at ikke alle funksjoner er tilgjengelig i den frie prøveversjonen.

Tilsvarende teknikker vil kunne benyttes ved distribusjon av annet opphavsrettslig vernet materiale, slik at kundens bruk i praksis blir begrenset. Filen kan være laget slik at den ikke kan kopieres videre, den kan låses til det utstyr den er installert på, osv.

Etter hvert vil det bygges identifikasjonsinformasjon inn i de digitale filene. Forkortelsen *DOI – Digital Object Identifier* kan man like godt lære seg først som sist. Dette kan være informasjon som identifiserer verket, samt informasjon om tillatt bruk av denne versjonen. Avspillingsutstyr vil så lese denne informasjonen, og vil ikke spille av filen dersom bruken er i strid med den rett brukeren har fått. Informasjonen vil kunne legges inn slik at det i

praksis ikke er mulig å fjerne den. Når man produserer en CD-plate samples lyden ca 44.000 ganger pr sekund. Det vil si at det lages så mange «snapshot» av lydbildet for hvert sekund, og dette settes sammen når lyden reproduseres. Om man tenker seg at det en gang pr sekund legges inn en DOI i stedet for et lydsignal, så vil det ikke være hørbart. Men det vil være meget vanskelig å fjerne fra koden.

Det vil bli forbudt å fjerne slik informasjon som identifiserer verket og brukes til administrasjon av rettigheter. Dette følger av *WIPO Copyright Treaty* fra 1996, og av artikkel 7 i det nye EF-direktivet om opphavsrett i informasjonssamfunnet, direktiv 2001/29/EF av 22. mai 2001.

Noen vil sikkert innvende at man aldri vil kunne hindre at noen bryter slike beskyttelsesmekanismer. Det er sikkert riktig. Men vissheten om at mange utviser stor kreativitet i sine forsøk på å smugle varer ulovlig inn i Norge hindrer ikke at vi har importrestriksjoner og tollkontroller. Og de fleste velger å benytte de legale kanaler – i alle fall hvis gevinsten ved ulovligheter ikke er for stor.

6 Avtaleregulering

Avtaler kan erstatte eller supplere det opphavsrettlige vernet. Sammenlignet med opphavsretten har avtaler imidlertid flere svakheter.

Den første begrensning i avtaleregulering er at avtalen bare binder de som er parter i avtalen. Jeg kan inngå en avtale med utgiver av denne artikkelen, som innebærer langt snevrere utnyttelsesrett enn det som følger av loven. Problemet er at jeg ikke har noen avtale med leserne, og leserne er ikke bundet av avtaler som utgiver måtte ha inngått med meg. En leser kan helt lovlig ta en kopi til privat bruk, selv om utgiver skulle ha inngått en avtale med forfatteren om at slik kopiering ikke skal finne sted.

En annen begrensning er at man bare er bundet av de vilkår som man var blitt presentert for og som man aksepterte da avtalen ble inngått. Hvis vi inngår en avtale, kan ikke jeg etterpå sende et brev med en rekke tilleggsvilkår som begrenser dine rettigheter, og hevde at du er bundet av disse. De var ikke med da avtalen ble inngått, og er ikke en del av avtalen. I praksis er det utenkelig at den enkelte kunde i en bokhandel skal bli presentert for et omfattende avtaledokument, som han så må lese igjennom mens kassekøen vokser bak ham. Derfor fungerer ikke individuell avtaleregulering i et tradisjonelt massemarked.

Når vi handler på nettet, kan kunden presenteres for omfattende avtaleregulering som må aksepteres før avtalen endelig inngås. At de fleste av oss aksepterer uten å lese igjennom vilkårene, er vårt problem. Det er ingen unnskyldning at man ikke leste igjennom vilkårene, og derfor ikke visste hva

avtalen gikk ut på. På denne måten har individuell avtaleregulering kommet inn igjen, og det brukes i betydelig grad.

Avtaler brukes til å regulere kundens rettigheter på måter som ikke kan bygge på opphavsretten, f eks begrensninger knyttet til bruk. Når slik avtaleregulering benyttes i kombinasjon med teknisk beskyttelse, vil produsentene kunne tvinge igjennom en beskyttelse som loven ikke gir grunnlag for, og som forskyver balansen i deres favør. Det vil også kunne bety at det er et selskap i USA som de facto bestemmer hva slags rettigheter norske kunder får, og ikke norske myndigheter etter mer eller mindre diktat fra Brussel.

7 Utfordringer ved nettdistribusjon av digitaliserte verk

Mange ønsker i dag å tilby informasjonsprodukter i digitalisert form via nettet. Det er f eks ingen tvil om at platebransjen ser at det her ligger store muligheter. Dagens distribusjon, hvor man sender tonnevis av plastikk rundt i verden, og hvor forhandlere binder kapital i å ha 50 – 100.000 titler på lager, er urasjonell og kostbar. Hvis man i stedet kan hente musikken via nettet, slipper man problemet med at titler er utsolgt eller ikke inngår i standard utvalget hos platebutikkene. Og man binder ikke kapital. At det samtidig betyr at grunnlaget for dagens platebutikker forsvinner, lar jeg i denne sammenhengen ligge.

Samtidig er det mange som er villige til å betale for informasjonsproduktene. I alle fall er vi villige til å betale dersom det i praksis ikke finnes noe alternativ, og prisen oppleves som rimelig. Vi betaler for abonnement på aviser, for CD-plater, for betalings-TV, for teletorg, osv. Man vil nok også betale for informasjon fra nettet, selv om mange vil knurre og klage over at det som tidligere har vært gratis ikke lenger er det. Dersom platebransjen gjør alt de sitter på tilgjengelig mot en rimelig betaling, vil de fleste av oss ikke finne det bryet verdt å lete etter pirattjenester med begrenset utvalg, som er vanskelig å finne fordi de stenges og/eller flytter, osv.

Platebransjen har nok skapt seg et problem ved at de alt for lenge var mer opptatt av å stritte i mot utviklingen frem enn å utnytte mulighetene. Det burde være et alvorlig tankekors for den bransjen at bokbransjen faktisk har kommet lenger. For mens mange holder fast ved at de vil lese tekst på papir som er bundet inn mellom to permer uten andre tekniske hjelpemidler enn briller for de av oss som trenger det, har vi alltid måttet ty til teknologiske hjelpemidler for å kunne nyte hermetisk musikk. Om dette innebærer at man putter en plastikkskive inn i en sprekk, eller laster den ønskede musikken ned fra nettet, burde ikke innebære noen vesentlig forskjell. Platebransjen har en stor utfordring i å hente inn igjen det piratmarked som har fått lov til å utvikle seg mens bransjen hadde hodet i sanden. Men det skjer nok etter hvert.

Det gjenstår fortsatt mye når det gjelder utvikling av teknologiske sikringsmetoder, slik at det blir vanskelig å omgå de begrensninger som kodes inn i filer som distribueres. Flere prosjekter har blitt stanset fordi sikkerheten har vist seg ikke å være god nok. Likevel er det nok ikke de teknologiske utfordringene som er størst.

Man trenger et organisatorisk apparat som gjør det enkelt for brukerne å finne det de måtte være interessert i, og å få klarert rettighetene til bruk av materialet. Det gjelder enten man ønsker rett til å se en film på sin TV-skjerm eller man vil bruke musikk som bakgrunn i en videoproduksjon. Det er nok en større utfordring å få etablert organisasjonen enn det er å få teknikken på plass.

Videre trenger man effektive betalingsløsninger. Vi vil ikke bruke tid på å inngå abonnementsavtaler eller andre former for rammeavtaler. Jeg vil kunne høre musikken her og nå, ikke om en uke når avtalen er på plass. Jeg vil heller ikke bruke tid på å betale småregninger, eller betale bankgebyrer som er høyere enn det beløp som skal betales. Det bør være like enkelt som når bruk av teletorgtjenester kommer på telefonregningen, og prisen for det som retter seg til vanlige forbrukere må ikke være høyere enn at man ikke er mer redd for å høre på musikk enn man er for å slå et telefonnummer.

Utvikling av slike systemer gir oss mange opphavsrettslige utfordringer. I tillegg gir det oss mange utfordringer innen kontraktsrett, personvernrett, internasjonal rett, konkurranserett, osv. Men det er temaer for flere nye artikler, og de skal få ligge i denne sammenhengen.

The technologisation of copyright: implications for privacy and related interests[1]

LEE A BYGRAVE

1 Introduction

A profound change is occurring in the way that intellectual property is protected. The change may be summed up as the technologisation of copyright. This somewhat inelegant phrase denotes the increasing use of technological mechanisms – including information systems architectures – to ensure that copyright is respected, particularly in the online environment. The basic purpose of this paper is to discuss the possible impact of this development on the privacy and related interests of users of information products. Only the basic contours of the issue are sketched here but it is hoped, nevertheless, to show that the issue warrants detailed discussion. For the issue is fundamental to determining the quality of life in the digital age.

The paper begins with an outline of the traditional interrelationship of copyright and privacy law. It then provides a brief description of the catalysts for the technologisation of copyright. Thereafter, an examination is made of how this technologisation might affect the privacy and related interests of information consumers. As part of the analysis, account is taken of certain legal instruments pertaining directly to the issue. The focus here is on the European Community (EC) Directive on copyright of 2001,[2] the United States (US) Digital Millenium Copyright Act of 1998,[3] and the EC Directive on data protection of 1995.[4]

---

1 This article is an extended version of an invited paper presented at the symposium, "Data Protection and Intellectual Property on the Internet", held in conjunction with the *Internationale Funkausstellung* in Berlin, 27.8.2001. The article has been accepted for publication in *European Intellectual Property Review*, vol 24, no 2.

2 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, pp 10 *et seq*.).

3 Public Law No 105-304 (1998), codified at 17 USC §§ 1201–1205 (1999).

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, pp 31 *et seq*.).

2 Copyright and privacy in the "good old days"

Copyright and privacy rights – broadly conceived – share a great deal in terms of their respective origins. Both have emerged to a considerable extent from doctrines on personality rights. This process has involved some cross-fertilisation of the two sets of interests: notions of copyright have helped to ground privacy rights, and notions of privacy have helped to ground copyright.[5]

This mutual aid has existed not just at the level of legal theory but also in practice. For instance, copyright law has furthered privacy interests by restricting publication of certain film material in which persons are portrayed,[6] and by restricting the ability of third parties to duplicate and further exploit lists of personal data compiled in certain registers.[7] Further, the exemptions to copyright in relation to the "private" or "fair" use of copyrighted material help to prevent copyright impinging unduly upon the private sphere of information consumers.[8] At the same time, privacy rights in the form of data protection law help copyright by placing limits on the processing of personal information that might subsequently be exploited in breach of copyright. Moreover, the respective agenda of copyright and privacy protection are similar, at least in their basic mechanics. Both attempt essentially to control the flow of information so as to safeguard certain values and interests.

Nevertheless, we should not overplay the similarities between their respective agenda. Nor should we overplay the extent to which the copyright community has taken privacy concerns actively into consideration and *vice-versa*. Any such consideration has been incidental and *ad hoc*. It is also apparent, for example, that the "private use" and "fair use" exemptions in copyright law are grounded not so much upon privacy considerations but on the interest of the wider community in gaining access to the fruits of creative endeavour.[9] Further, the privacy of consumers of copyrighted material has clearly been due to a range of factors that have little to do with copyright law.[10] Pro-

5 See, eg, S Warren & L Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review*, pp 193 *et seq*, especially p 198 (arguing, *inter alia*, that common law protection of intellectual, artistic and literary property is based upon a broader principle of protection of privacy and personality).

6 See, eg, UK Copyright, Designs and Patents Act 1988 (as amended), s 85(1); Australia's federal Copyright Act 1968 (as amended), s 35(5); Norway's Intellectual Property Act 1961 (*lov om opphavsrett til åndsverk mv 12. mai 1961 nr 2*; as amended), s 45c. For further discussion, see S Theedar, "Privacy in photographic images" (1999) 6 *Privacy Law & Policy Reporter*, pp 75–78.

7 See, eg, the decision of the Federal Court of Australia in *Telstra Corporation Limited v Desktop Marketing Systems Pty Ltd* [2001] FCA 612, 25 May 2001 in which Telstra Corporation Limited was found to hold copyright in the white and yellow page databases which it publishes. The case caused the shutdown of a reverse phone directory service ("blackpages") operated by a third party. The service covered major cities in Australia. Given a phone number, it was able to find the name and address of the owner.

8 See further LA Bygrave & KJ Koelman, "Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems", in PB Hugenholtz (ed), *Copyright and Electronic Commerce* (2000), pp 59, 99 *et seq*.

bably the most important of these factors has been that sales of copyrighted material have usually been able to be carried out as anonymous cash transactions and that the material itself has lacked mechanisms to monitor and report on its usage.

Equally clear is that the concerns of copyright differ in fundamental respects from the concerns of privacy and data protection. Put somewhat simplistically, the steering axiom for data protection advocates is "knowledge is power". For copyright-holders, a steering axiom of greater importance is "knowledge is wealth". More particularly, copyright is an attempt to protect the incentive to produce original works and contribute to public well-being by assuring the creators an economic benefit of their creative activity.[11] By contrast, data protection attempts to maintain the incentive to participate in a democratic, pluralist society by securing the privacy, autonomy and integrity of individuals.[12]

3 The digital dilemma – and responses

Any tensions that have existed between copyright and privacy rights as a result of the differences in their respective agenda, have been kept largely in abeyance up until recently. Now, however, a significant tension between the two sets of rights is emerging in the context of cyberspace. This tension arises not so much from the core natures of either set of rights. Rather, it arises from a particular response of copyright-holders to what is often termed the "digital dilemma".[13] The "digital dilemma" with respect to copyright springs from the fact that the digital environment (including the technology that creates that environment) brings a greatly increased ability to copy information in breach of copyright.

---

9 Note, though, that privacy considerations have figured in certain decisions of the German Federal Supreme Court (*Bundesgerichtshof*) limiting the ability of copyright-holders to monitor and prohibit private/domestic audio-recording practices. In this regard, see *Personalausweise* decision of 25 May 1964 [1965] GRUR 104; *Kopierläden* decision of 9 June 1983 [1984] GRUR 54. For other examples where privacy considerations appear to have played some role in setting boundaries for copyright, see Bygrave & Koelman, *ibid*, pp 102–103 and references cited therein.

10 For an overview of these factors, see G Greenleaf, "'IP, Phone Home': ECMS, ©-Tech, and Protecting Privacy against Surveillance by Digital W*orks", in Proceedings of the 21st International Conference on Privacy and Data Protection* (1999), pp 281, 282–283.

11 See generally JAL Sterling, *World Copyright Law* (1998), pp 57–61.

12 See generally LA Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (forthcoming), Chapter 7 and references cited therein.

13 See, eg, Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applicatons; National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age* (2000).

The response by the copyright community to this threat has been, firstly, to conclude (indeed, to a great extent, *assume*) that the pre-existing balance of power struck between the interests of copyright-holders and the interests of information users, has shifted radically in favour of the latter. From this conclusion (or assumption) has flowed a second conclusion, which is that traditional user rights under copyright law need to be rolled back significantly. The result has been a vigorous campaign for reform of copyright law to strengthen the rights of copyright-holders at the expense of user rights, at least in relation to digital artefacts.

4 Technologisation

The push for legal reform has been accompanied by increasing recognition that "the answer to the machine is in the machine" – to quote the now rather worn phrase of Clark.[14] Expressed alternatively using Lessig's terminology,[15] the copyright community has become evermore aware of the important ways in which "code" or information systems architecture regulates how information can be used, and it has become determined to exploit these regulatory abilities for the protection of intellectual property. Thus, we see the development of a range of technological (and, to some extent, organisational) mechanisms to help secure copyright in digital artefacts. Taken together, these mechanisms have tended to go under the name of Electronic Copyright Management Systems; more recent terminology refers increasingly to Digital Rights Management Systems (DRMS).

In a nutshell, such systems provide an infrastructure allowing the creator of an information product to enforce copyright in the product when it is accessed online by other parties. This facility breaks down into several overlapping functions, the most central of which are, in summary:

- controlling access to information products;
- preventing the unauthorised copying of the products;
- identifying the products and those who own copyright in them; and
- ensuring that the latter identification data are authentic.

14 C Clark, "The Answer to the Machine is in the Machine", in PB Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (1996), pp 139–148.
15 See generally L Lessig, *Code, and Other Laws of Cyberspace* (1999).

Realisation of these functions is envisaged as being built around a variety of copyright-protective technologies involving, *inter alia*, steganography (eg, digital watermarking for authentication of identification data), encryption (eg, for controlling access to information products) and various electronic agents (eg, web spiders for monitoring information usage).[16]

Currently, though, there is a paucity of fully operational DRMS involving all of the above functionalities.[17] Hence, much uncertainty still surrounds the exact ways in which they will operate.

The technologisation of copyright has a parallel in the field of privacy and data protection, where there is also increasing recognition of the need to create technological mechanisms that ensure respect for privacy interests particularly in the online world. These mechanisms go often under the name of Privacy-Enhancing Technology (PETs).[18] However, PETs have yet to receive the same sort of statutory backing as copyright-protective technologies are receiving – a point returned to further below.

5 Privacy implications

While uncertainty still surrounds the exact means and parameters of DRMS operations, little doubt exists that they will have the potential of amassing a great deal of data about the persons who purchase usage rights to information products. They will also have the potential of registering data about persons who merely *browse* – ie, who inspect or sample information products without purchasing a particular right with respect to them. In both cases, data could be registered which are normally not registered in conjunction with ordinary shopping transactions effectuated in "meatspace". Hence, a DRMS could facilitate the monitoring of what people privately read, listen to, view or sample, in a manner that is more comprehensive than what hitherto has been usual.[19] This surveillance potential would be augmented, of course, if a DRMS were

16 For a relatively detailed overview of these mechanisms, see Greenleaf, *supra* n 10, pp 284–288. See also, eg, DS Marks & BH Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences" [2000] EIPR, pp 198 *et seq*, especially pp 212–213; KJ Koelman & N Helberger, "Protection of Technological Measures", in PB Hugenholtz (ed), *Copyright and Electronic Commerce* (2000), pp 165, 166–169; Koelman & Bygrave, *supra* n 8, pp 60 – 61, 108–110.

17 For examples of existing systems, see DJ Gervais, "Electronic Rights Management and Digital Identifier Systems" (1998) 4 *Journal of Electronic Publishing*, Issue 2, at <http://www.press.umich.edu/jep/04-03/gervais.html> (last visited 6.11.2001).

18 For an overview, see, eg, H Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision", in PE Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997), pp 125–142.

19 See further JE Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 *Connecticut Law Review*, pp 981 *et seq*; Bygrave & Koelman, *supra* n 8; Greenleaf, *supra* n 10.

integrated with other information systems so that the monitoring data could readily be combined with data about persons' activities in other contexts, thus enabling the composition of fine-grained personal profiles.

This potential could not only weaken the privacy interests of information consumers to an unprecedented degree but also inhibit the expression of non-conformist opinions and preferences.[20] Thus, a DRMS could function as a kind of digital Panopticon. This eventuality has unsettling implications for the long-term health of pluralist, democratic society. It remains to be seen just how effectively data protection laws will be able to reign in such an eventuality – a point dealt with further below.

6 Other problematic consequences – w(h)ither the soul of copyright?

A DRMS will also have the potential to reduce the autonomy of information consumers in another, less subtle way by enabling the ready imposition of predetermined licensing conditions on information usage. There is a danger that such conditions will undercut the exemptions from copyright which traditionally are provided under copyright law (eg, for private use of information products). As Koelman notes, this danger is also attributable to the current limitations in the ability of technology itself to take due account of the numerous lawful copyright exemptions – "[t]echnology – at this stage – is simply too crude to accommodate all the subtleties of the law".[21] The danger could be augmented by the enactment of legal rules restricting the circumvention of copyright-protective technologies even in cases when these technologies render nugatory the lawful copyright exemptions.[22]

The technologisation of copyright has troubling implications not just for the autonomy and privacy of information users but also for broader social discourse. Knowledge is increasingly structured and distributed by digital information systems. Thus, the technologisation of copyright will increasingly impinge on knowledge flows. Concomitantly, how technologisation

20 *Ibid*.

21 KJ Koelman, "The protection of technological measures vs. the copyright limitations", Paper presented at the ALAI Congress, "Adjuncts and Alternatives for Copyright", New York, 15 June 2001, at <http://www.ivir.nl/publications/koelman/alaiNY.htm>.

22 See further, eg, TC Vinje, "Copyright Imperilled?" [1999] EIPR, pp 192, 197 *et seq*; JE Cohen, "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them" (1997) 12 *Berkeley Technology Law Journal*, pp 161 *et seq*, especially pp 179 *et seq*. Note too criticism of the efficacy of the EC copyright Directive of 2001 (particularly Art 6(4)) in countering this danger: see, eg, TC Vinje, "Should We Begin Digging Copyright's Grave?" [2000] EIPR, pp 551, 556–558; PB Hugenholtz, "Why the Copyright Directive is Unimportant, and Possibly Invalid" [2000] EIPR, pp 499, 500.

occurs is vitally important for the quality of social discourse, particularly the extent to which we are able to maintain "digital diversity" and a broad public domain.[23] An aggressive technologisation of copyright could seriously impair the flow of knowledge throughout society, with the impoverishment of social discourse as a further result.

Additionally, technologisation will have consequences for the long-term status of copyright law. It is likely to facilitate the use of contract as the primary means of regulating usage of copyrighted material,[24] thus helping to marginalise traditional copyright law in favour of contract law – at least in the digital context. In broader terms, this is a development in which enforcement of intellectual property rights increasingly relies on private fiat, decreasingly on public law with its finely tuned balance of interests.[25]

Finally, the technologisation of copyright will have profound consequences for the way in which copyright is perceived by the community at large – a point that has not been sufficiently emphasised in policy discussions to date. The push by copyright-holders to pre-emptively secure copyright in ways that greatly impinge on the privacy and autonomy of information consumers, is leading to accusations of regulatory overreaching.[26] Lending strength to such accusations is the trend by legislators to give strong statutory backing to copyright-protective technologies – a development returned to further below. Also lending strength to such accusations is the failure by copyright-holders to adequately supply empirical justification for their claim that they shall be ripped off to an unprecedented degree if they do not apply copyright-protective technologies and obtain extensive statutory support for these. There already exists considerable antipathy or indifference to copyright amongst many information consumers. The perception of regulatory overreaching which comes in the wake of technologisation exacerbates these attitudes and fosters a crisis of legitimacy for the copyright industry.

To sum up so far, the technologisation of copyright could well have troubling consequences for the privacy and autonomy of information users. It could also have troubling consequences for the long-term status of, and

---

23 See further B Fitzgerald, "Intellectual Property Rights in Digital Architecture (including Software): The Question of Digital Diversity" [2001] 23 EIPR, pp 121–127. See also, eg, PB Hugenholtz, "Code as code, or the end of intellectual property as we know it" (1999) *Maastricht Journal of European and Comparative Law*, pp 308, 316 *et seq* and references cited therein.

24 As Hugenholtz aptly notes, "technological measures will be applied mostly in combination with contract": *ibid*, p 312.

25 See further, eg, CEA Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law* (1997), chapter 3; TC Vinje, "A Brave New World of Technical Protection Systems: Will There Still be Room for Copyright?" [1996] EIPR, pp 431 *et seq*, especially p 437.

26 See, eg, Hugenholtz, *supra* n 23, pp 314–315; P Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised" (1999) 14 *Berkeley Technology Law Journal*, pp 519 *et seq*.

respect for, copyright law. Indeed, one is tempted to say that, with extensive technologisation, copyright could well end up losing its soul.

7 The copyright Directive

The use of copyright-protective technologies is being afforded strong statutory support. In Europe, this support is provided primarily by Articles 6 and 7 of the copyright Directive passed in 2001, and more indirectly by Articles 11 and 12 of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996.[27] Article 6 of the Directive stipulates, in summary, that adequate legal protection shall be provided against the intentional circumvention of any effective "technological measures" (ie, copyright-protective technologies). Article 7 of the Directive stipulates, in summary, that adequate legal protection shall be provided against: (a) the intentional and unauthorised alteration or removal of "electronic rights management information"; and (b) the distribution of copyrighted works from which such information has been removed or altered, in the knowledge that such distribution breaches copyright. Articles 11 and 12 of the WIPO Copyright Treaty (WCT) are broadly similar to these provisions. In the following, focus is put on the Directive rather than the WCT.

The above provisions are complex and raise numerous issues of interpretation.[28] Two such issues are broached in this opinion. Both concern directly the privacy-invasive potential of copyright-protective technologies.

The first issue is whether the concept of "technological measures" in Article 6 of the Directive (and Article 11 of the WCT) extends to devices that monitor usage of copyrighted information. If such devices are not covered, then their disablement will not constitute a breach of Article 6(1). This, of course, would be the most privacy-friendly result. If such devices are covered, their disablement will, *prima facie*, violate Article 6(1), though the violation could perhaps be legitimised pursuant to data protection law. Note that Article 9 of the Directive states that its provisions shall be without prejudice to legal provisions in other areas, including data protection and privacy. As indicated further below, however, the efficacy of data protection law in this context is unclear.

---

27 See too the mirroring provisions in Articles 18 and 19 of the WIPO Performances and Phonograms Treaty of 1996.

28 For analysis of some of these issues, see, eg, KJ Koelman, "A Hard Nut to Crack: The Protection of Technological Measures" [2000] 22 EIPR, pp 272–280; Koelman & Helberger, *supra* n 16, pp 169 *et seq*; AME de Kroon, "Protection of Copyright Management Information", in PB Hugenholtz (ed), *Copyright and Electronic Commerce* (2000), pp 229, 250 *et seq*.

The Directive itself provides no obvious answer to the issue. This is also the case with the WCT. However, there can be little doubt that some monitoring devices are covered, given the broad way in which "technological measures" is defined in the Directive – ie, as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts [in breach of copyright] …" (Article 6(3)). At the same time, the requirement that the device be concerned with copyright protection in the *normal* course of its operation, could be taken to mean that monitoring devices which are only *incidentally* concerned with such protection fail to qualify as technological measures. This would be the case, for example, with ordinary devices for the setting of so-called "cookies" and/or "web bugs" (also termed "1-pixel gifs"). One might also query whether devices that *merely* carry out monitoring tasks (albeit with copyright protection as the primary purpose) can properly be viewed as "designed to prevent or restrict" breaches of copyright. However, it is easier to argue that monitoring *per se* can have the requisite preventative/restrictive function – indeed, to argue otherwise would ignore the increasingly self-evident control dynamics that are central to the notion of panopticism.

It is instructive to compare Article 6 of the Directive with section 1201(i) of the US Digital Millenium Copyright Act (DMCA). The latter provision permits the disabling of *access controls* upon certain conditions:

1. the access controls collect or disseminate information about the online activities of a person;
2. conspicuous notice about this information processing is not given;
3. the data subject is not provided the ability to prevent the information being gathered and disseminated; and
4. the disabling of the controls has the sole effect, and is solely for the purpose, of preventing the collection and dissemination.

This provision seems clearly aimed at allowing for the disabling of ordinary "cookies"-mechanisms and "web bugs" (if all of the above conditions apply). However, doubts have been raised about its application to other monitoring devices that are more integral to copyright-protective technologies.[29] Its practical utility is also questionable given that the DMCA restricts the supply of tools that could disable the access controls in question.[30]

The second issue concerns the scope of what the copyright Directive terms "rights management information" (RMI). More specifically, the issue is

29 See Samuelsen, *supra* n 26, pp 553 *et seq*.
30 DMCA, s 1201(a)(2) and (b)(1).

whether personal data relating to a consumer of copyrighted information are to be treated as a necessary component of RMI. The issue is important because if such data are *not* to be treated as a necessary component, alteration or erasure of such data by an information consumer cannot fall foul of Article 7(1).

The term RMI is defined in Article 7(2) as including "information about the terms and conditions of use of the [copyrighted] work or other subject matter". The same pertains to the definition of RMI in Article 12(2) of the WCT. Does information about "terms and conditions of use" necessarily include personal data about the users of copyrighted works? Does it necessarily include personal data relating to how the works are used? The expression "terms and conditions of use" does not, *prima facie*, comfortably embrace such data.[31] However, given that some information usage licences may be quite user-specific, it is arguable that such data may be covered.[32] Support for this argument can also be derived from recital 57 in the preamble to the Directive which recognises that RMI-systems may "process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour".

By contrast, section 1202 of the US DMCA specifically defines "copyright management information" (the equivalent to RMI) as excluding digital information used for monitoring usage of copyrighted works. Again, the US legislation appears at first blush to be more privacy-friendly than the Directive.[33]

If personal data about information users are to be treated as a component of RMI, the removal or alteration of such data will only breach Article 7(1) if the act concerned is unauthorised. The requisite authority may probably be derived from legislation, particularly legislation on privacy/data protection.[34] The question then becomes whether and to what extent alteration or erasure of the data is actually permitted or required pursuant to data protection laws. This is a difficult question: the answers to it will tend to vary from jurisdiction to jurisdiction and depend on the outcome of complex, relatively open-ended interest-balancing processes that hinge considerably on an assessment

---

31 Bygrave & Koelman (*supra* n 8, p 115) claim accordingly that such data appear not to be covered by the definition of RMI in the WCT.

32 This is also the line taken by Greenleaf, *supra* n 10. Bygrave and Koelman (*ibid*) recognise this possibility too.

33 This is not to say, though, that information consumers in the USA therefore enjoy generally more legal protection for their privacy than information consumers in Europe do. It is probably more accurate to say that, on the whole, legal protection for information consumers' privacy is more extensively and systematically built up in European jurisdictions than it is in the USA. The apparent disparity is partly evidenced by the "safe harbor" agreement which was concluded in July 2000 between the USA and EU and which stipulates conditions for permitting the flow of personal data from the EU to the USA.

34 See also de Kroon, *supra* n 28, p 254. Note too Article 9 referred to in the main text above.

of what information processing is "necessary" in the particular circumstances of the case.[35]

In Europe, the most important privacy safeguards in this respect will have to be derived primarily from the EC Directive on data protection, together with national laws implementing it. The Directive will permit the non-consensual registration and further processing of data on consumers of copyright-protected works if, in summary, the processing is necessary for the performance of a contract or for the establishment, exercise or defence of legal claims or for realising legitimate interests that outweigh the privacy interests at stake.[36] If these conditions are construed liberally, information consumers will find it difficult to have legitimately removed or altered the data about them registered by DRMS operators.

Recital 57 in the copyright Directive stipulates that "technical" privacy safeguards for such data "should" be incorporated in accordance with the data protection Directive. Thus, the recital goes some way to encouraging the use of PETs. However, from a privacy perspective, recital 57 is disappointing. It is disappointing for three reasons.

First, it seems to link the use of PETs only to the design and operation of RMI-systems, not also to the design and operation of the technological measures referred to in Article 6. This is rather incongruous as the ongoing monitoring of information usage is most likely to occur through the application of these technological measures.[37] Certainly, data protection rules and measures may still apply in the context of Article 6 – particularly given Article 9 – but it would have been preferrable for the Directive to encourage more directly the use of PETs in that context too.

Secondly, recital 57 appears not to mandate the use of PETs. It states only that privacy safeguards "should", not "shall", be incorporated.

Thirdly, the reference in the recital to the data protection Directive is problematic because that Directive fails to specifically address the use of PETs.[38] Moreover, the data protection Directive has very little to say about the desirability of transactional anonymity or even pseudonymity. Certainly, parts of the Directive – particularly Articles 6 to 8 stipulating the basic conditions for

35 See further the extensive analysis of European data protection rules in Bygrave & Koelman, *supra* n 8, especially pp 75–97.

36 *Ibid*, pp 75–78. More stringent conditions apply for the processing of certain categories of especially sensitive personal data, though exactly which types of data would fall within these categories in a DRMS context is somewhat unclear: *ibid*, pp 78–81.

37 Further, as Dusollier points out, the definition of RMI in Art 7 as information "provided by rightholders", does not accurately apply to the situation in which information usage is actively monitored; such monitoring will rather occur as an automatic function of a technological measure referred to in Art 6. See S Dusollier, "Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright" [1999] EIPR, pp 285, 296.

38 Perhaps this is why recital 57 does not mandate PET application.

when personal data may be processed – can be read as encouraging transactional anonymity,[39] but this encouragement is far from direct. By contrast, German federal legislation on data protection contains relatively far-reaching provisions specifically mandating transactional anonymity and, to some extent, pseudonymity.[40] It is to be hoped that the German approach inspires greater legislative support for transactional anonymity and pseudonymity in other jurisdictions too.

More generally, several question marks hang over the extent to which data protection laws will apply to DRMS operations. These question marks arise not just because of continuing uncertainty about how DRMS will function in practice but also because of uncertainty about the ambit of data protection laws in a digital context. Perhaps the most significant issue here relates to the fact that data protection laws tend to apply only when data are personal – ie, can be linked to identifiable natural/physical persons. It is to be expected, though, that DRMS operations will involve to a considerable degree the processing of so-called "clickstream" data that are primarily linked to the Internet protocol (IP) addresses of computers. The extent to which such data may qualify as personal data for the purposes of data protection law is still being worked out.[41] Moreover, it is to be expected that DRMS will involve, to a large extent, the use of various types of electronic agents – ie, software applications which, with some degree of autonomy, mobility and learning capacity, execute specific tasks for a computer user or computer system. Again, the way in which the operations of these agents may fall within the ambit of data protection legislation is only just beginning to be systematically considered.[42]

8 Considerations for the future

A problem with much of the debate about the implications of new forms of copyright protection is that it is accompanied by a large degree of uncertainty. As this paper highlights, uncertainty reigns on many fronts. There is uncertainty about the parameters and *modus operandi* of DRMS; uncertainty about the ambit and application of legal rules with respect to both copyright

39 See further Bygrave, *supra* n 12, chapter 18.

40 See particularly §§ 3(4), 4(1), 4(4) and 6(3) of the Teleservices Data Protection Act (*Teledienstedatenschutzgesetz*) of 1997. Also noteworthy are the recently enacted provisions on "Datenvermeidung" and "Datensparsamkeit" in § 3a of the 1990 Federal Data Protection Act (*Bundesdatenschutzgesetz*) as amended in May 2001.

41 For preliminary discussion of the issue, see G Greenleaf, "Privacy principles – irrelevant to cyberspace?" (1996) 3 *Privacy Law & Policy Reporter*, pp 114–115; Bygrave & Koelman, *supra* n 8, pp 72–73; Bygrave, *supra* n 12, chapter 18.

42 For a preliminary analysis, see LA Bygrave, "Electronic Agents and Privacy: A Cyberspace Odyssey 2001" (2001) 9 *International Journal of Law and Information Technology*, pp 275 *et seq*.

and data protection; and uncertainty about the impact of market mechanisms. Hence, the debate is largely based on assumptions about potentialities. This is an important point to bear in mind.

Indeed, current concerns about the technologisation of copyright might end up being largely unsubstantiated. We might be conjuring up a threatening mountain out of what proves to remain a molehill. Several factors could serve to hinder the large-scale implementation of privacy-invasive DRMS. Such systems might be marginalised by market mechanisms – for example, strong consumer preferences for privacy, combined with competition between copyright-holders to satisfy these preferences.[43] The take-up of privacy-invasive DRMS might also be hindered by difficulties in achieving standardisation and compatibility of technological measures.[44]

These uncertainties notwithstanding, future policy must aim to prevent copyright-protective mechanisms from knocking down privacy and related interests through technological fiat or one-eyed lobbying on the part of copyright-holders. Such interests should not be sacrificed given their importance for the vitality of democratic, pluralist society.

Moreover, if copyright-protective mechanisms trample over privacy, it is highly likely that copyright-holders will lose financially if not in other ways. Copyright is easier to swallow if it is seen as respecting users' privacy and autonomy. Further, copyright-holders should benefit if electronic commerce takes off, and electronic commerce is likely to take off only if consumer privacy is seen to be protected. Considerable evidence exists to indicate that numerous consumers are reluctant to enter into online commercial transactions because they fear for their privacy.[45]

A second objective should be to work towards a better integration of technological measures for protecting copyright with PETs. As noted above, the technologisation of copyright has a parallel in the technologisation of privacy and data protection. This parallel should be exploited for the benefit of privacy and data protection. A large range of technological and organisational mechanisms exist to enforce copyright in a digital environment. Some are more privacy-invasive than others. We need to encourage the development and application of the least privacy-invasive devices. Such encouragement is actually required already by some laws, particularly in Germany, and it arguably follows, though more indirectly, from the data protection Directive.

---

43 See also Samuelsen, *supra* n 26, pp 565–566. Cf Hugenholtz, *supra* n 23, p 312 (noting previous instances of the market marginalisation of certain anti-copying devices because of their irritation to consumers).

44 There exists a myriad of competing standards with respect to the structuring and provision of RMI. See further Gervais, *supra* n 17.

45 See, eg, A Bhatnagar, S Misra & H Raghav Rao, "On Risk, Convenience, and Internet Shopping Behavior" (2000) 43 *Communications of the ACM*, pp 98 *et seq*.

Bevisbruk under straffesak av opplysninger innhentet ved kommunikasjonskontroll eller infiltrasjon

– en krenkelse av den menneskerettslig beskyttede taushetsretten?

JENS PETTER BERG

1 Problemstilling

Høsten 1999 vedtok Stortinget ett nytt kapittel 16 a i straffeprosessloven som hjemler avlytting og annen kontroll av kommunikasjonsanlegg bl a i saker hvor noen med skjellig grunn mistenkes for en handling som etter loven kan medføre straff av fengsel i 10 år eller mer.[1] Disse bestemmelsene trådte i kraft 15.10.2000.

I den grad det var politisk strid om disse lovbestemmelsene, dreide den seg hovedsakelig om hva slags straffbare handlinger som skulle kunne hjemle bruken av et så inngripende tvangsmiddel. Få, om overhodet noen røster hevet seg mot forslaget om å endre skrankene for hva de innhentede opplysningene skulle kunne brukes til. Etter de tidligere gjeldende lovreglene var den tillatte bruken av opplysninger fra kommunikasjonskontroll begrenset til etterforskningsbruk, f eks spaning, ransaking og beslag. Den nye strpl § 216i(1)(b) har fjernet denne skranken. Nå tillates det at opplysninger innhentet ved kommunikasjonskontroll også framlegges under hovedforhandlingen som bevis for straffeskyld.

Det er uomstridt at politiets kommunikasjonskontroll regnes som et inngrep i borgernes sfære internrettslig sett, og derfor ikke kan skje uten lovhjemmel. En slik politimetodebruk er også utvilsomt i utgangspunktet en krenkelse av Den europeiske menneskerettskonvensjon (EMK) art 8(1) om vern av retten til respekt for privatlivet mv, som bare er konvensjonsforenlig dersom unntakskriteriene i art 8(2) er oppfylt.

I fortsettelsen er det ikke disse aspektene ved politiets kommunikasjonskontroll jeg er opptatt av. Isteden vil jeg løfte fram en hittil neglisjert konsekvens for mistenkte/tiltalte av politiets bevisbruk av opplysninger innhentet

1 Lov av 3.12.1999 nr 82. Forarbeider er NOU 1997: 15, Ot prp nr 64 (1998–99) og Innst O nr 3 (1999–2000).

ved kommunikasjonskontroll: nemlig at slik bevisbruk reelt sett må bedømmes som en krenkelse av den straffeprosessuelle – og menneskerettslige beskyttede – taushetsretten.

Bevisbruk av opplysninger innhentet gjennom politiets *infiltrasjon* i kriminelle miljøer reiser likeartede rettsspørsmål som bevisbruk av opplysninger fra kommunikasjonskontroll. Infiltrasjon har i Norge tradisjonelt vært regnet som en politimetode som kan skje uten lovhjemmel. Også spørsmålet om politiets bruk av infiltrasjon som sådan må betraktes som en krenkelse av EMK art 8(1), har hittil knapt vært debattert. På de følgende sider problematiserer jeg følgelig også disse aspektene ved politiets bruk av infiltrasjon som arbeidsmetode.

2 Taushetsretten og vernet mot sjølinkriminering – rettigheter som gir substans til uskyldspresumsjonen i straffesaker

Mistenktes taushetsrett i straffesaker er ikke bare under press som følge av økende bruk av kommunikasjonskontroll og politiinfiltrasjon: Vår forrige justisminister (Hanne Harlem) klandret våren 2001 landets forsvarere for å gi sine klienter det råd å nekte å forklare seg overfor politiet. Etter terrorangrepene mot USA 11.9.2001 har det innen amerikansk påtalemyndighet blitt tatt til orde for å innføre tortur som avhørsmetode i amerikansk straffeprosess. Dette er eksempler på at mange justisaktører i vår tid har glemt at den *frie* bevisbedømmelsen i straffeprosessen opprinnelig betød *torturfri* bevisbedømmelse.[2] Torturfriheten signaliserte en sivilisasjonsutvikling hvor beslutningstakerne hadde frigjort seg fra den nærmest animistiske forestillingen at tiltaltes ubetingede skyldinnrømmelse var nødvendig for å kunne avsi en fellende straffedom. Som operasjonelt uttrykk for torturforbudet fikk vi en rekke straffeprosessuelle bestemmelser som fastslo *mistenktes og tiltaltes taushetsrett* overfor politi og domstoler, bestemmelser som nå er nedfelt bl a i strpl §§ 90, 92(2) første setning og 232, jf også påtaleinstruksen kapittel 8.

Noenlunde samtidig med revolusjoneringen av bevisretten slo *uskyldspresumsjonen* gjennom – som en sentral frukt av opplysningstida og en byggestein i forestillingen om den liberale rettsstaten. Etter dette prinsippet skal mistenkte anses som uskyldig inntil påtalemyndigheten har bevist det motsatte utover rimelig tvil. Et kasuistisk uttrykk for dette prinsippet finner vi nå i voteringsregelen i jurysaker (strpl § 372). For øvrig er prinsippet ulovfestet hos oss.[3] I

2 Torturforbudet i Grl § 96 andre setning, vedtatt i 1814, formaliserer den revolusjon av bevisretten som da allerede hadde slått gjennom i norsk rettsvesen.

de sentrale menneskerettsinstrumentene er derimot uskyldspresumsjonen ikke oversett. Vi finner den allerede i Verdenserklæringen om menneskerettighetene (VE) art 11(1), og ellers i EMK art 6(2) og i FN-konvensjonen om sivile og politiske rettigheter (SP) art 14(2).

Taushetsretten er ikke noen logisk nødvendighet i en straffeprosessordning med uskyldspresumsjon. Alle siviliserte stater anerkjenner imidlertid i dag taushetsretten som en moralsk nødvendighet i en slik straffeprosessordning.

Vernet mot sjølinkriminering – mistenktes og tiltaltes beskyttelse mot tvang til enten å vitne mot seg sjøl eller å erkjenne straffeskyld – er en av taushetsrettens viktigste konkrete manifestasjoner. Denne rettigheten har tilflytt menneskerettssamfunnet gjennom angloamerikansk rettsutvikling.[4] Det er et paradoks at verken VE eller EMK inneholder uttrykkelige bestemmelser om dette vernet; en slik formalisering skjedde først gjennom SP art 14(3)(g). I løpet av 1990-tallet ble likevel vernet mot sjølinkriminering etter praksis fra EMK-organene forankret i *fair hearing*-standarden i EMK art 6(1).[5]

3 Presentasjon av den nye bestemmelsen i strpl § 216i(1)(b) om bevisbruk under straffesak av opplysninger fra kommunikasjonskontroll

Den nye bestemmelsen i strpl § 216i, i kraft 15.10.2000, tillater for det første at opplysninger innhentet ved kommunikasjonskontroll brukes som utgangspunkt for iverksetting av ytterligere etterforskningsskritt mot den mistenkte, se § 216i(1)(a). For det andre tillater bestemmelsen også at opplysningene framlegges under straffesak som bevis for straffeskyld, se § 216i(1)(b). Bevisbruk under straffesak av opplysninger fra kommunikasjonskontroll innebærer en 180 graders snuoperasjon i forhold til det tidligere gjeldende – i 1992 innførte[6] – uttrykkelige forbudet mot at opplysninger fra telefonavlytting i narkotikasaker framlegges *som bevis* for straffbart forhold.[7]

Under forberedelsen av 1992-loven hadde politiet og påtalemyndigheten av etterforskningstaktiske grunner anbefalt at opplysninger fra telefonavlyt-

---

3 Etter mitt syn må uskyldspresumsjonen utvilsomt regnes blant de uskrevne, semikonstitusjonelle grunnrettighetene i den norske rettsordningen, jf nærmere herom min artikkel i *KJ* 2000 s 129–44.

4 I USAs forfatning er sjølinkrimineringsvernet inntatt i *Bill of Rights, Fifth Amendment* fra 1791.

5 Grunnleggende er her *Funke mot Frankrike* 25.2.1993 *Series A* No 256-A, *Murray mot England* 8.2.1996 *RJD* 1996-I og *Saunders mot England* 17.12.1996 *RJD* 1996-VI. En interessant dom fra i år, som uttrykkelig bygger på *Murray mot England*, er *Telfner mot Østerrike* 20.3.2001 *RJD* 2001-? (ennå ikke trykt).

6 Lov av 5.6.1992 nr 52, se Ot prp nr 40 og Innst O nr 61 (1991–92).

7 Se tidligere strpl § 216i(3), slik bestemmelsen lød etter lov av 5.6.1992 nr 52.

ting utelukkende skulle betraktes som et *etterforskningsmiddel*. Ved at opplysningene som slik framkom utelukkende skulle kunne gi grunnlag for iverksetting av andre etterforskningsskritt (ransaking, beslag osv), ville man først og fremst avverge at det ble nødvendig å framlegge etterforskningstaktiske opplysninger, herunder opplysninger om kilder og tips, under hovedforhandlingen. Videre ville man unngå det man omtalte som en vidløftiggjøring av bevisførselen under hovedforhandlingen.

Denne holdningen hadde politiet og påtalemyndigheten inntatt bl a under trykket fra høyesterettsavgjørelsene i Rt 1991 s 1018 og Rt 1991 s 1142, som klargjorde at påtalemyndigheten ikke kunne føre opplysninger fra telefonavlytting som bevis, uten samtidig å gi tiltalte fullt partsinnsyn. Betenkelighetene mot å tillate bevisbruk av opplysninger fra telefonavlytting ble sammenfattet slik av Justisdepartementet:

> «… Det har vært adgang til å foreta telefonkontroll i 15 år, og det er bare i en håndfull saker påtalemyndigheten har benyttet lydbånd eller utskrifter av lydbånd som bevis under hovedforhandlingen. ... Det er med andre ord bare i helt spesielle tilfeller at påtalemyndigheten ønsker å benytte telefonkontrollopplysningene som bevis under hovedforhandlingen.»[8]

I NOU 1997: 15 (Metodeutvalget) hadde imidlertid politi og påtalemyndighet endret holdning, liksom i 1992 under påberopelse av etterforskningstaktiske argumenter. Denne holdningsendringen ble utslagsgivende også for Justisdepartementet. Nå ble dessuten både hensynet til det materielle sannhetsprinsippet og prinsippet om fri bevisbedømmelse framhevet som begrunnelse for å endre lovbestemmelsen.[9]

Som konsekvens av denne holdningsendringen ble de tidligere bestemmelsene om å nekte mistenkte partsinnsyn i dokumenter vedrørende telefonkontrollen foreslått opphevet.[10] Mistenkte og/eller hans forsvarer har nå på etterforskningsstadiet i hovedsak samme krav på innsyn i relevante saksopplysninger vedrørende kontrollen som i straffesaker ellers (strpl § 242), og dersom tiltale reises, vil de i utgangspunktet ha et ubetinget krav på slikt innsyn (strpl § 264, jf § 292).

Når Den Norske Advokatforening under høringen om NOUen uttrykte at bevisbruk av opplysninger fra kommunikasjonskontroll er uproblematisk, så sant mistenkte/tiltalte og hans forsvarer får innsyn i det samlede bevismaterialet, har foreningen naturligvis hatt sitt hovedfokus på *våpenjevnbyrdighetsprinsippet*. At mistenkte/tiltalte må gis partsinnsynsrett i alt

---

8 Ot prp nr 40 (1991–92) s 32 første spalte andre avsnitt.
9 Ot prp nr 64 (1998–99) avsnitt 8.7 s 64 flg. Justisdepartementets egen vurdering står på s 66 flg.
10 Se tidligere strpl § 216 i (4), og § 216 j (2) siste setning, slik bestemmelsene lød etter lov 5.6.1992 nr 52.

materiale som framkommer ved kommunikasjonskontroll, dersom påtalemyndigheten ønsker å bruke deler av dette som bevis under straffesaken, har støtte i praksis fra EMK-organene om dette prinsippets forankring i EMK art 6(1), og politiets/påtalemyndighetens forsøk på å nekte slikt partsinnsyn i åra før 1992-lovendringen måtte rimeligvis derfor før eller seinere møte veggen i Høyesterett. Dessverre har imidlertid advokatforeningens fokusering på våpenjevnbyrdighetsprinsippet tatt oppmerksomheten bort fra konsekvensene for mistenktes/tiltaltes taushetsrett av de nye reglene om bevisbruk av opplysninger fra kommunikasjonskontroll. Disse spørsmålene ble derfor overhodet ikke berørt av foreningen. Mer om dette i avsnitt 5 nedenfor.

4 Det tradisjonelle norske synet på bevisbruk under straffesak av opplysninger innhentet gjennom infiltrasjon

Det har lenge vært en utbredt oppfatning i Norge – med særlig rotfeste i påtalemyndigheten og ellers i visse kretser i Justisdepartementet – at politiets bruk av infiltrasjon som kriminaletterretningsmetode, og iallfall bruk av infiltrasjon i forbindelse med etterforskning av allerede utførte straffbare handlinger, ikke som sådan trenger lovhjemmel. I proposisjonen til straffeprosessloven av 1981 ble spørsmålet om lovregulering av sjølve metodebruken streifet av Justisdepartementet i tilknytning til drøftelsen av et foredrag[11] av daværende riksadvokat LJ Dorenfeldt om behovet for å lovregulere såkalt «etterforskning med provokasjonstilsnitt» i narkotikasaker. I likhet med Dorenfeldt tilrådde departementet å overlate skrankesettingen på dette feltet til domstolene, og justiskomiteen hadde ingen merknader til dette.[12]

Det synet at infiltrasjon, på samme måte som den beslektede kriminaletterretningsmetoden *spaning* (observasjon), ikke trenger lovhjemmel, springer ut av den – etter mitt syn høyst besynderlige – vurdering at disse metodene normalt ikke representerer noe *inngrep i borgernes sfære*. I NOU 1997: 15 uttalte utvalget således, med direkte adresse til spaning:

> «Utgangspunktet er at spaning ikke krever hjemmel i lov. Men spaningen kan tenkes å bli så intensiv at det ... vil være tale om et inngrep i den private sfære som etter legalitetsprinsippet krever hjemmel i lov. *Det skal imidlertid svært mye til før denne grense passeres ved politiundersøkelser.* Kjernen i all spaning er at den forutsettes å være passiv. I den grad politi-

11 Trykt i *LoR* 1978 s 291–303.
12 Ot prp nr 35 (1978–79) s 179, Innst O nr 37 (1980–81) s 26 første spalte første avsnitt.

> tjenestemenn som spaner utviser en form for aktivitet i forhold til det miljøet det spanes på, vil spaningen kunne gli over i infiltrasjon.»[13]

Som det ses, var man i dette Metodeutvalget, som foruten vår nåværende riksadvokat Tor-Aksel Busch besto av et knippe av våre fremste påtalemyndighets- og politiledelsesjurister, ikke ukjent med at legalitetsprinsippet setter skranker for politiets ikke uttrykkelig hjemlede bruk av kriminaletterretningsmetoder. I en ellers svulmende utredning fant man imidlertid ikke grunn til å gå nærmere inn på de tvilsspørsmål som kunne melde seg, f eks når spaning foretas fra steder som ikke er allment tilgjengelig.

Heller ikke Justisdepartementets lovavdeling fant grunn til å gå nærmere inn på lovhjemmelsproblematikken i tilknytning til bruken av spaning og infiltrasjon som arbeidsmetoder i politiet i lovproposisjonen om politimetoder:

> «Departementet er enig med Metodeutvalget i at det for tiden ikke er grunn til å innføre generelle regler om spaning og infiltrasjon. Det er her i første rekke tale om *mer tradisjonelle etterforskningsmetoder* som ikke er så inngripende at det er behov for lovregulering…»[14]

Det er verdt å merke seg formuleringen om at infiltrasjon i utgangspunktet regnes blant de mer tradisjonelle etterforskningsmetodene. Dette er i kontrast til bruk av infiltrasjon *i kombinasjon med* provokasjon, det Dorenfeldt på 1970-tallet hadde betegnet som «etterforskning med provokasjonstilsnitt», som i påtalemyndighetsjargong regnes som en «ekstraordinær» etterforskningsmetode.

I de gjengitte tilnærminger sondres det ikke mellom infiltrasjon brukt som verktøy for ytterligere etterforskningsskritt (f eks ransaking eller beslag), og infiltrasjon brukt som bevisframskaffelsesmetode.

Heller ikke for Høyesterett har spørsmålet om infiltrasjonens lovlighet *per se* noen gang kommet på spissen. I forhold til spørsmålet om hva infiltrasjon lovlig kan nyttes til har lovligheten bare blitt behandlet i situasjoner hvor politiet har *framprovosert* det aktuelle beviset for en straffbar handling, slik at dette aspektet ved politiets metodebruk har fått all oppmerksomhet.

Den fortsatt grunnleggende rettsavgjørelsen i denne sammenheng er dommen i Rt 1984 s 1076, hvor førstvoterende dommer Aasland, under henvisning til regjeringen og Stortingets uvilje mot å lovgi på feltet, formulerte den setning at skrankene for det lovlige, i mangel av positiv lovgivning, må «bero på slike alminnelige rettsprinsipper som ligger til grunn for vår strafferettspleie» (s 1079 nestsiste avsnitt). I forlengelsen av dette formulerte så dommer Aasland den skranke at «det ikke kan aksepteres at politiet fremkaller en

13 NOU 1997: 15 s 80 første spalte fjerde og femte avsnitt. Min kursivering.
14 Ot prp nr 64 (1998–99) s 122 avsnitt 16.1.4 første underavsnitt. Min kursivering.

straffbar handling som ellers ikke ville ha blitt begått» (s 1080 tredje avsnitt). Hva dette betyr konkret, foreligger det etter hvert en nokså rikholdig høyesterettspraksis om. I alle disse sakene har det omtvistede rettsspørsmålet vært formulert som et bevisavskjæringsspørsmål, altså om bevis kan tillates ført for straffbare handlinger, dersom disse er framprovosert av politiet, med den underforståtte følge at tiltalte må frifinnes for tiltalen, dersom beviset nektes ført.[15] Denne rettspraksisen går jeg ikke nærmere inn på her, fordi den ikke tar stilling til det reindyrkede spørsmålet om bevisbruk under straffesak av opplysninger innhentet gjennom infiltrasjon.

Den 6.7.2001 nedsatte regjeringen Stoltenberg et utvalg under ledelse av førstelagmann Odd Jarl Pedersen for å vurdere lovregulering av politiets metoder for å *forebygge* kriminalitet, altså politiets *proaktive* bruk av spaning, infiltrasjon mv i situasjoner hvor det ennå ikke er etablert et tilstrekkelig mistankegrunnlag for iverksetting av etterforskning etter strpl § 224(1). I mandatet for utvalget, som er utarbeidet av Justisdepartementets lovavdeling, er den finske lovgivningen på feltet framhevet som særskilt interessant å dra lærdom av. Jeg ser på nedsettingen av Pedersen-utvalget som et høyst påkrevet tiltak for å avhjelpe at Justisdepartementet ikke sørget for at slik lovregulering kom på plass allerede i forbindelse med stortingsbehandlingen våren 2001 av de nye lovbestemmelsene om overvåkingstjenestens oppgaver, jf Ot prp nr 29 og Innst O nr 89 (2000–2001).

Norsk lovregulering av politiets kriminaletterretningsmetoder, både den proaktive og den reaktive bruken, synes i dag å være klart akterutseilt i forhold til flere av statene i Europa det er naturlig å sammenlikne oss med. Dette gjelder særlig i forhold til tysk lovgivning, men også i forhold til dansk lovgivning. I begge disse land har man hatt en langt klarere forståelse enn hos oss av nødvendigheten av å ha en klar lovmessig forankring av politiets metodebruk innenfor sitt kjernearbeidsfelt, etterforskning av straffbare handlinger. For eksempel fremmet regjeringen i Danmark allerede 8.10.1998 et forslag for Folketinget (L 41) om lovregulering i retsplejeloven av flere inntil da ulovregulerte kriminaletterretningsmetoder under etterforskning, herunder offentlig etterlysning, forevisning av fotografier av mistenkte til personer utenfor politiet og spaning i form av «fotografering eller iagttagelse ved hjælp af kikkert eller andet apparat af personer, der befinder sig på et ikke frit tilgængeligt sted (observation)». Lovforslaget ble vedtatt av Folketinget 13.4.1999 med brei tilslutning, men er ikke nevnt i Justisdepartementets mandat for Pedersen-utvalget.

15 Se henholdsvis Rt 1992 s 1088, Rt 1993 s 473, Rt 1998 s 407 (skrik), Rt 1998 s 1269 (fengselsbetjent), Rt 2000 s 1223, Rt 2000 s 1345 og Rt 2000 s 1482.

5 Bevisbruk under straffesak av opplysninger fra kommunikasjonskontroll eller infiltrasjon vurdert i forhold til den straffeprosessuelle taushetsretten

Når politiet og påtalemyndigheten gjennom bestemmelsen i strpl § 216i(1)(b) har fått lovhjemmel for å kunne benytte bl a hemmelige opptak av telefonsamtaler, og datautskrifter av e-post og SMS-meldinger, som bevis i straffesaker, er enkeltindividenes handlefrihet med hensyn til fortrolig kommunikasjon blitt betydelig innsnevret. Betroelsesrelasjoner som man før trygt kunne regne med som beskyttet av uskrevne og skrevne diskresjonsregler, er nå potensielt en kommunikasjonssituasjon hvor politiets lange ører lytter med. Når borgerne ytrer seg per telefon, e-post eller ved SMS-meldinger, må de heretter forholde seg som om de satt i et politiavhør, dvs ta høyde for at alt de sier kan bli brukt mot dem som bevis i en straffesak, med den vesentlige forskjell i forhold til et ordinært politiavhør at ingen politietterforsker gir et forhåndsvarsel om retten til å forholde seg taus ved starten av samtalen. Konsekvensene av den nye strpl § 216i(1)(b) er mao at vår tids mest egnede fora for borgernes utfoldelse av sine betroelsesrelasjoner er omskapt til *funksjonelle politiavhørsfora*.

Det er mitt håp at verken regjeringen eller Stortinget har skjønt denne konsekvensen av lovendringen, og heller ikke har overskuet at lovendringen trolig krenker EMK-kravene til norsk straffeprosesslovgivning. Dermed er det meningsfylt å forsøke å bidra til en slik forståelse.

Jeg vil da først framheve at Høyesterett allerede noen få måneder før justiskomiteen avga sin innstilling om den nye strpl § 216i(1)(b), i den såkalte fengselsbetjentdommen, Rt 1999 s 1269, avgjorde at påtalemyndigheten ikke har lov til å framlegge lydbåndopptak som bevis mot tiltalte i straffesak, når opptaket inneholder en erkjennelse av en straffbar handling, og erkjennelsen er *framprovosert* i samtale med en polititjenestemann eller en person som står i ledtog med politiet.

Den aktuelle straffesaken gjaldt en fengselsbetjent A som var tiltalt for å ha hjulpet narkoforbryteren B med å rømme fra Ullersmo landsfengsel. Som ledd i en politifelle var betjenten blitt lokket til å tilby en annen innsatt C på Ullersmo, som samarbeidet med politiet, rømningsbistand. Det var herunder blitt avtalt at A skulle overlevere en skisse av fengselet til en medsammensvoren av C utenfor en dagligvarebutikk, mot et vederlag på kr 80 000. Den medsammensvorne var i virkeligheten politibetjent D, som utstyrt med skjult båndopptaker framprovoserte en forklaring fra A, hvor denne skal ha innrømmet å ha hjulpet til med Bs rømning og gitt en nærmere forklaring på hvordan det skjedde. Det var opptaket fra denne samtalen som ble ført som bevis i straffesaken mot A.

Førstvoterende dommer Skoghøy, med tilslutning av dommerne Matningsdal, Lund, Tjomsland og justitiarius Smith, uttalte bl a:

> «I vår sak dreier det seg om etterforskningsskritt som tar sikte på å fremprovosere forklaring fra siktede, og for slike etterforskningsskritt gjør særlige hensyn seg gjeldende. Det er et grunnleggende rettsstatsprinsipp at den som er mistenkt for en straffbar handling, har rett til å forholde seg taus, og ikke har noen plikt til å bidra til egen straffellelse. ... også lenge før [SP og EMK] ble gjort til norsk rett, har det vært et grunnfestet prinsipp for norsk straffeprosess at den som er mistenkt for en straffbar handling, ikke har noen forklaringsplikt. ... I dette tilfellet er A ved politiets bruk av C og politibetjent D blitt forledet til å forklare seg om den befatning som han etter politiets syn skal ha hatt med Bs rømning. Dette skjedde uten at A selv hadde invitert til kontakt med C og D. Etter min mening har politiet ved den fremgangsmåte som er blitt benyttet, ikke i tilstrekkelig grad respektert mistenktes rett til å forholde seg taus.»[16]

Ut fra denne høyesterettsdommen er det når det gjelder bevisbruk av opplysninger fra kommunikasjonskontroll eller infiltrasjon på det reine at man under enhver omstendighet må sondre mellom mistenktes/tiltaltes «spontane» innrømmelser, som altså presumptivt fortsatt *kan* være lovlige bevis, og de framprovoserte innrømmelsene, som heretter mål regnes som ulovlige bevis.

Fengselsbetjentdommen kaster etter mitt syn på en treffende måte lys over en grunnleggende svakhet ved Justisdepartementets tilnærming til spørsmålet om å tillate bevisbruk av opplysninger innhentet gjennom kommunikasjonskontroll – at man ikke har foretatt noen egentlig overveielse av konsekvensene for mistenktes/tiltaltes taushetsrett. Dersom dette var blitt gjort, er det nærliggende å tro at man ville ha valgt å fastholde ordningen som ble lovbestemt i 1992, altså at bruken av slike opplysninger begrenses til annen etterforskingsbruk.

Støtte for et slikt resonnement ville Justisdepartementet ha funnet, dersom man hadde gått nærmere inn på EMK-rettslig argumentmateriale. Det foreligger riktignok neppe noen enkeltavgjørelse fra EMD som direkte uttaler at det strir mot uskyldspresumsjonen i EMK art 6(2) eller taushetsretten som er innfortolket i art 6(1) å bruke opplysninger fra kommunikasjonskontroll eller infiltrasjon som bevis i straffesak. Det er likevel etter mitt syn gode holdepunkter for å hevde at bestemmelsen i strpl § 216i(1)(b) som tillater generell bevisbruk av opplysninger fra kommunikasjonskontroll, ikke er i overensstemmelse med den *sannsynlige utviklingsretningen* i det menneskerettslige vernet av den straffeprosessuelle taushetsretten.

Et eksempel fra de seinere åra på hvordan taushetsrettens rekkevidde etter EMK art 6 er blitt trengt noe i bakgrunnen til fordel for mer lettfattelige, og dermed enklere prosedable, problemstillinger, er EMDs dom *Teixeira de*

16 Rt 1999 s 1269 på s 1271 nestsiste avsnitt flg.

Castro mot Portugal[17], som gjaldt en narkotikasak hvor det var blitt nyttet etterforskning med provokasjonstilsnitt. Her ble Portugal med stemmetallet 8–1 felt for å ha krenket rettferdig rettergang-standarden i art 6(1). Flertallet kritiserte ikke bruken av politiinfiltrasjon som sådan, men at infiltratøren hadde gått for langt – ved å gjennomføre en salgsprovokasjon (forbrytelsesprovokasjon). EMDs flertall la nemlig avgjørende vekt på at forbrytelsen, salget av 20 gram heroin, ikke ville ha skjedd dersom politiinfiltratøren ikke hadde tilskyndet til handelen. Avgjørende for domsutfallet, som er helt i tråd med norsk domspraksis på dette feltet,[18] var altså salgsprovokasjonen, ikke at infiltrasjon var blitt nyttet som arbeidsmetode.

Mitt syn er at infiltrasjon er en kriminaletterretningsmetode som krenker taushetsretten etter EMK art 6(1) *ved proaktiv bruk*, dvs uten at det er etablert skjellig grunn til mistanke om at en straffbar handling er begått, dersom informasjonen som erverves gjennom infiltrasjonen nyttes til iverksetting av etterforskningsskritt. Da har nemlig politiet i realiteten vært på såkalt «fisketur», dvs etablert det jeg foran kalte et funksjonelt politiavhørsforum uten et tilstrekkelig mistankegrunnlag. *Nyttet reaktivt*, dvs som ledd i etterforskning ved mistanke om straffbart forhold, vil infiltrasjon av samme grunn være en krenkelse av taushetsretten etter art 6(1), dersom informasjonen som innhentes brukes som bevis for straffbare handlinger, og ikke bare som hjelpemiddel for iverksetting av andre etterforskningsskritt, herunder tvangsmiddelbruk som f eks ransaking og beslag.

Bruk av opplysninger fra kommunikasjonskontroll som bevis i straffesak må etter mitt syn i forhold til taushetsretten etter EMK art 6(1) bedømmes på samme måte som bevisbruk av opplysninger innhentet ved hjelp av infiltrasjon. Reelt sett etablerer kommunikasjonskontrollen en funksjonell avhørssituasjon, dersom mistenktes «spontane» kommunikasjonsytringer tillates nyttet som bevis mot den mistenkte.

I en klasse for seg må man uansett bedømme den nye strpl § 216 l, likeledes i kraft 15.10.2000, som ved skjellig grunn til mistanke om en handling som etter loven kan gi frihetsstraff, gir politiet rett til «ved teknisk innretning» (mikrofon eller båndopptaker) å avlytte eller gjøre opptak av telefonsamtale med den mistenkte, dersom politiet enten sjøl deltar i samtalen eller har fått samtykke til avlyttingen (lydopptaket) fra den mistenktes samtalepartner. Bestemmelsen har en kuriøs forhistorie: en nær samlet justiskomité hadde ca 10 år tidligere i kjølvannet av den såkalte møbelhandler-saken pålagt regjeringen å utrede spørsmålet om å gi en straffebestemmelse rettet mot slike opptak av telefonsamtaler man sjøl deltok i.[19]

17 9.6.1998 *RJD* 1998-IV.
18 Se avsnitt 4 foran, med fotnote 15.

I lovproposisjonen viste Justisdepartementet i denne forbindelsen bl a til at EMD-dommen *A mot Frankrike*[20] gjorde det nødvendig med lovhjemmel iallfall for opptak av telefonsamtale som tredjemann i samråd med politiet hadde med mistenkte, for at hjemmelskravet etter EMK art 8(2) skal være oppfylt.[21] Justisdepartementet streifet imidlertid bare såvidt den problemstillingen som kom på spissen i fengselsbetjentdommen, Rt 1999 s 1269, nemlig at telefonsamtalen kan utvikle seg slik at den reelt sett får karakter av å være et politiavhør, og den mistenkte derfor har krav på å få vite dette, samt å bli underrettet om sin rett til å nekte å forklare seg. Etter fengselsbetjentdommen er det derfor klart at domstolene, uten hensyn til det som står i strpl § 216 l, må avskjære bevisframleggelse dersom det er nyttet provokasjon under telefonsamtalen for å få fram en tilståelse, eller telefonsamtalen ellers reelt sett må bedømmes som et fordekt politiavhør.

6 Politiets infiltrasjon i narkotikamiljøer og i prategrupper mv på internettet vurdert som krenkelse av retten til respekt for privatliv og familieliv mv etter EMK art 8

At infiltrasjon som kriminaletterretningsmetode i utgangspunktet må regnes som en krenkelse av retten til respekt for privat- og familieliv eller korrespondanse, slik denne er vernet etter EMK art 8(1), er etter mitt syn en nokså sikker oppfatning. For EMK-organene har i sin tolkingspraksis generelt lagt terskelen lavt for å konstatere at det har skjedd et inngrep («interference») i den konvensjonsbeskyttede rettigheten etter denne artikkelen.

Riktignok kjenner jeg ikke til noen enkeltdom eller kommisjonsuttalelse som tar direkte stilling til dette spørsmålet, men inngrepsterskelen er drøftet i en rekke liknende saker. Jeg framhever som eksempel EMD-dommen *Niemietz mot Tyskland*[22], en sak om lovligheten av ransaking på et advokatkontor. Her

---

19 Se Ot prp nr 56 (1989–90) og Innst O nr 25 (1990–91), kjent som *lex Engen*, etter den besynderlige historien om møbelhandleren på Jessheim som hadde samlet båndopptak av telefonsamtaler med en rekke ledende DNA-politikere gjennom flere år. Instruksen som Stortinget ga regjeringen, hadde visse kretser i Justisdepartementet og påtalemyndigheten liten sans for. Først etter sju år ble derfor saken fremmet på ny, nå med forslag om å droppe både det opprinnelige lovforslaget om å strafflegge offentliggjøringen av telefonsamtaler man sjøl deltok i, samt stortingsflertallets ønske om å strafflegge også sjølve båndopptaket av telefonsamtalene. Se Ot prp nr 55 (1997–98) og Innst O nr 28 (1998 - 99). Også på Stortinget hadde stemningen i mellomtida snudd, og regjeringens nye forslag ble vedtatt uten debatt.

20 23.11.1993 *Series A* No 277-B.

21 Ot prp nr 64 (1998–99) s 84–87.

22 16.12.1992 *Series A* No 251-B.

gikk domstolen langt i retning av å tolke EMK art 8(1) som et generelt vern mot inngrep i borgernes sfære.

Saken hadde sin opprinnelse i en straffesak mot en arbeidsgiver som hadde nektet å trekke sine ansatte for kirkeskatt. I forkant av denne saken hadde dommeren mottatt et brev fra en fiktiv person (Klaus Wegner) på vegne av partiet «Bunte Liste» («flerfarget liste») i Freiburg, som sympatiserte med denne arbeidsgiveren, hvor det bl a ble tatt avstand fra at dommeren hadde truffet beslutning om tvungen psykiatrisk undersøkelse av vedkommende arbeidsgiver. Domstolens justitiarius ba påtalemyndigheten om å iverksette etterforskning for å finne opphavsmannen til brevet, som ble oppfattet som injurierende. Seinere traff retten beslutning om å gjennomføre ransaking av bl a kontoret til klageren, den tyske advokat G. Niemietz, som hadde vært det nevnte partiets leder, og fortsatt mottok post på dettes vegne, med sikte på å få klarhet i hvem som skjulte seg bak den fiktive personidentiteten.

Det som er interessant her, med sikte på å avgjøre om infiltrasjon *som sådan* kan være en krenkelse av art (1), er både at EMD gikk langt i å tolke denne artikkelen som et generelt vern mot inngrep fra myndighetene i borgernes sfære, og at ordet «home» også ble ansett å omfatte et advokatkontor:

> «*More generally, to interpret the words 'private life' and 'home' as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 …, namely to protect the individual against arbitrary interference by the public authorities* ... Such an interpretation would not unduly hamper the Contracting States, for they would retain their entitlement to 'interfere' to the extent permitted by paragraph 2 of Article 8 ...; that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case.»[23]

Grunnen til at EMK-organene neppe har tatt stilling til om *politiinfiltrasjon som sådan* må regnes som en krenkelse av art 8(1), er trolig så enkel at infiltrasjonens karakter av krenkelse av retten til respekt for privat- og familieliv først blir kjent for de krenkede dersom politiet gjennom infiltrasjonen skaffer seg bevis for straffbare handlinger, som enten kan brukes til iverksetting av andre etterforskningsskritt (f eks ransaking og beslag), eller framlegges direkte som bevis i straffesak. Dermed kommer bevisframleggingens lovlighet, ikke infiltrasjonens lovlighet, på spissen for domstolene nasjonalt – og for EMK-organene.

---

23 Avsnitt 31; min kursivering. EMD felte enstemmig Tyskland i denne saken, med den grunngiving at ransakingsbeslutningen var så generelt formulert at ransakingen måtte regnes som et uforholdsmessig inngrep, og derfor ikke kunne aksepteres som hjemlet i nasjonal rett etter EMK art 8(2).

Når infiltrasjon brukes av politiet som etterforskningsmetode, er formålet unntaksfritt å framskaffe bevis for straffbare handlinger som allerede er begått, eller med utgangspunkt i slike handlinger å kunne avverge at nye straffbare handlinger begås. *Innhenting og lagring av personopplysninger* er mao et sentralt delformål med infiltrasjonshandlingen. Om innhenting og registrering av personopplysninger i forbindelse med *proaktiv* eller *reaktiv politisk overvåking* foreligger det en rekke avgjørelser fra EMK-organene. Jeg skal her trekke fram en av de aller ferskeste, *Amann mot Sveits*[24], som gjaldt en sveitsisk næringsdrivende som under den kalde krigen var blitt registrert av overvåkingspolitiet av den banale grunn at en russisk diplomat hadde kjøpt én av varene han forhandlet, et hårfjerningsapparat, fra ham.

EMD startet med å rekapitulere – under henvisning til *Leander mot Sverige*[25] – at «storing of data relating to the 'private life' of an individual falls within the application of» EMK art 8(1).[26] Med hensyn til spørsmålet om lagringen som sådan utgjorde en krenkelse av art 8(1), uttalte domstolen deretter:

> «The Court reiterates that the storing by a public authority of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding…»[27]

At EMD var av den oppfatning at allerede lagringen av personopplysninger, her det sveitsiske overvåkingspolitiets lagring av et kartotekkort med opplysninger om klageren, i seg sjøl var en krenkelse av art 8(1), er ikke egnet til å overraske. Men EMD gikk lenger. Som svar på den sveitsiske regjeringens anførsel om at Amann verken var blitt krenket («inconvenienced») ved utfyllingen («the creation») eller lagringen av kartotekkortet, fordi kortet ikke inneholdt noen sensitive opplysninger om ham, og trolig aldri hadde blitt sett på av utenforstående, uttalte dommerne:

> «In the instant case the Court notes that a card containing data relating to the applicant's private life was filled in by the Public Prosecutor's Office and stored in the Confederation's card index. In that connection it points out that it is not for the Court to speculate as to whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way. It is sufficient for it to find that data relating to the private life of an individual was stored by a public

24 16.2.2000 *RJD* 2000-I.
25 26.3.1987 *Series A* No 116 avsnitt 48.
26 *Amann mot Sveits* 16.2.2000 *RJD* 2000-I avsnitt 65 første underavsnitt.
27 Avsnitt 69.

> authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life.»[28]

Etter min vurdering er det med utgangspunkt i disse uttalelsene fra Amanndommen gode grunner til å regne bruk av politiinfiltrasjon som en krenkelse av art 8(1), fordi en vellykket infiltrasjon nettopp kjennetegnes ved at personene i miljøene som det infiltreres i, ikke merker infiltrasjonen. I en slik situasjon har det like fullt skjedd en *invadering i de involverte privatliv*, med sikte på å *utnytte det etablerte tillitsforholdet* for polisiære formål.

I løgndetektorkjennelsen, Rt 1996 s 1114, brukte førstvoterende dommer Schei nettopp en variant av *invadering i privatliv*-formuleringen som den avgjørende begrunnelsen for å avskjære adgangen til å føre bevis fra løgndetektortest i en straffesak om forsikringsbedrageri:[29]

> … [Løgndetektortesten] skal ... avsløre et 'kroppsspråk' som ikke kan kontrolleres, og den vil ved dette innebære en *invadering av personligheten* ved at sannheten fås fram uten at testpersonen har kontroll over det.[30]

Det å kunne stole på hverandre i betroelsesrelasjoner er udiskutabelt helt grunnleggende for etableringen av tillits- og vennskapsbånd mellom mennesker, og dermed for samfunnnsetablering i det hele tatt. Evnen til å stole på hverandre er også et kjerneaspekt ved det som i fortalen til Verdenserklæringen om menneskerettighetene er betegnet som «recognition of the inherent dignity» (anerkjennelsen av den iboende verdighet) til alle mennesker. Taushetsplikten i betroelsesrelasjoner, med skriftemålshemmeligheten og legenes taushetsplikt som de eldste, nedtegnede eksemplene, er et krystallklart uttrykk for alle kultursamfunns vilje til å verne om de sensitive personopplysningene som utveksles i slike sammenhenger.

En infiltrasjonshandling framtrer som en ubetinget grovere integritetskrenkelse enn en kommunikasjonskontrollhandling, da denne skjer uten at den som rammes, utsettes for noen ansikt til ansikt-kontakt med en polititjenesteperson. På bakgrunn av at det i årevis har vært udiskutabel enighet om at lovhjemmel trengs for å kunne foreta kommunikasjonskontroll, framstår det som forbløffende at noen kan hevde at politiinfiltrasjon i miljøer som mistenkes for å romme kriminelle personer, ikke skal regnes som et inngrep i borgernes sfære.

---

28 Avsnitt 70.

29 Det var tiltalte som i denne saken hadde tatt initiativ til å føre beviset, fordi det talte til hans fordel, mens påtalemyndigheten ville avskjære bevisførselen. Sjøl en slik konstellasjon avverget ikke Høyesterett fra å vende tommelen ned for bruk av løgndetektortesten på et prinsipielt grunnlag.

30 Side 1119 tredjesiste avsnitt. Min kursivering.

At formålet med en politiinfiltrasjon like fullt *kan* være beskyttelsesverdig, hensett til de antatt straffbare forholds alvorsgrad, er udiskutabelt, men like fullt *irrelevant* ved avgjørelsen av om infiltrasjonshandlingen innebærer en krenkelse av retten til respekt for privat- og familielivet etter art 8(1). For å løse de interesseavveiningsspørsmålene som slik reiser seg, har nemlig EMKs konsipister satt inn et eget unntaksavsnitt i artikkelen – art 8(2). Artikkel 8(2) åpner for et vidt spekter av begrensninger i eller unntak fra privatlivsbeskyttelsen etter art 8(1), forutsatt at disse unntakene (a) har forankring i nasjonal rett, (b) er uttrykk for et påtrengende samfunnsmessig behov[31] og (c) ikke er uforholdsmessige. Praksis fra EMK-organene bærer gjennomgående preg av at man har gått rett løs på drøftelsen av om disse inngrepskriteriene er oppfylt, og tatt det for gitt at inngrepet ellers er en krenkelse av art 8(1). Også etter en slik generell betraktning vil man da nærmest uten videre legge til grunn at politiinfiltrasjon som sådan er en krenkelse av art 8(1). Det er nemlig en typisk lovgiveroppgave å avgjøre hvilke områder av borgernes livsutfoldelse i det sivile samfunn som bør forbli skjermet mot politiinfiltrasjon, og hva som konkret skal være «trigger»-mekanismene for lovliggjøring av slike politimetoder.

I Norge har det, som nevnt i avsnitt 2 foran, vært en utbredt oppfatning at politiets bruk av infiltrasjon som ledd i etterforskningen av straffbare handlinger i utgangspunktet kan skje uten særskilt lovhjemmel, og dette spørsmålet har ikke Høyesterett tatt stilling til i rein form. Riksadvokaten har ut fra dette syn standhaftig valgt å hemmeligholde de rundskriv som i de siste 20 åra er utferdiget om bruk av infiltrasjon som etterforskningsmetode, under påberopelse av bl a offvl § 6(1)(2c). Både Den norske advokatforening og jeg sjøl har i flere år forgjeves forsøkt å få innsyn i disse rundskrivene, og særlig rundskriv av 9.3.1998 og 2.10.1998 om politiinfiltrasjon henholdsvis i narkotikamiljøer og på internettet.[32]

Det er hevet over tvil at lovskravet etter EMK art 8(2) ikke er oppfylt av Norge, dersom infiltrasjon i narkotikamiljøer og på nettet regnes som et inngrep i borgernes rett til respekt for deres privatliv og familieliv etter art 8(1). Hemmelige inngrepshjemler er nemlig blant de groveste eksemplene på krenkelser av EMK. Hva angår de nærmere kravene som i praksis fra EMK-organene er blitt oppstilt til inngrepshjemlers tilgjengelighet og klarhet/forutsigbarhet, nøyer jeg med å vise til standardlitteraturen om emnet.[33]

---

31 Oversettelsen til norsk av ordene «pressing social need» følger her Høyesteretts oversettelse i Rt 1997 s 1821 (Kjuus-kjennelsen) på s 1829 siste avsnitt, som jeg tror er den beste som hittil er foretatt.

32 Mine innsynsanmodninger er først blitt neglisjert, og deretter blitt avslått. Seinest 20.7.2001 har Justisdepartementets politiavdeling gitt Riksadvokaten støtte for det standpunktet at disse rundskrivene kan unntas fra offentlighet. Se brev m/ref 97/8915 PPU/MSv til Sivilombudsmannen, som tilsvar til min klage av 24.4.2000 (sak nr 2000-0734 B). Sivilombudsmannens endelige uttalelse i saken foreligger ennå ikke når dette skrives (primo november 2001).

EMK-organenes krav om at det aktuelle inngrepet etter en konkret vurdering ikke må framtre som uforholdsmessig, innebærer etter min vurdering at EMK art 8(2) utvilsomt gir den enkelte et vern mot å bli utsatt for politiinfiltrasjon, med mindre en slik metodebruk dokumenteres å være et påtrengende samfunnsmessig behov i det aktuelle tilfellet. En mer detaljert grensedragning mellom konvensjonsforenlig og konvensjonsstridig infiltrasjon etter forholdsmessighetskriteriet i art 8(2) er vanskelig. Jeg skal ikke her gå inn på drøftelse av konkrete eksempler. Det er høyst beklagelig i denne sammenheng at Riksadvokatens hemmeligholdelse av rundskrivene om politiinfiltrasjon ikke engang gjør det mulig å vurdere den *generelle* forholdsmessigheten av politiets infiltrasjonspraksis.

33 Se f eks Per Lorenzen m fl: *Den Europeiske Menneskeretskonvention* (1994), s 48 flg.

Vilkår for å sette bort systemutviklingsoppgaver som omfatter myndighetsutøvelse[1]

DAG WIESE SCHARTUM

1 Forholdet mellom forskriftsmyndighet, myndighet til å treffe rettslige systemavgjørelser og myndighet til å treffe enkeltvedtak

Når en utvikler edb-baserte beslutningssystemer (heretter «beslutningssystemer»), skjer dette gjerne primært på grunnlag av lover og forskrifter (det vil si på grunnlag av generelle vedtak), og som en forberedelse til å treffe enkeltvedtak. Denne forberedelsen kan sies å gå ut på å identifisere materielle og prosessuelle rettslige spørsmål som kan avgjøres på forhånd, det vil si avgjøre rettsspørsmål uavhengig av konkrete saker. Slike avgjørelser betegner jeg «rettslige systemavgjørelser». De rettslige systemavgjørelsene uttrykkes deretter i datamaskinprogrammer, noe som gjør det mulig å automatisere deler av myndighetsutøvelsen.

Når en skal gjennomføre rettslige analyser av beslutningssystemer, er det et grunnleggende problem å beskrive den myndighetsutøvelse som skjer som ledd i systemutviklingen. Innen forvaltningsretten opererer en gjerne med to hovedtyper av beslutninger som er rettet mot folk utenfor forvaltningsorganet selv: Noe forenklet uttrykt er «enkeltvedtak» slike vedtak som avgjør konkrete enkeltpersoners rettsforhold, mens «forskrifter» avgjør rettsforhold for en ubestemt gruppe personer, se forvaltningsloven (fvl) § 2 bokstavene b og c, jf bokstav a.

I rettsteorien har det vært diskutert om programkode som inneholder rettslige systemavgjørelser, kan anses å være «forskrifter» i forvaltningslovens forstand, se Rynning (1976) , Bing (1977), Schartum (1989) og Eckhoff/Smith (1999, s 545). I så fall ville fvl kap VII gjelde for de «rettslige systemavgjørelser» som treffes innenfor rammene av systemutviklingsarbeidet, og således bli gjenstand for høring og kunngjøring. Selv har jeg, med tilslutning fra

1 Artikkelen er tidligere publisert (med noen små redaksjonelle endringer) som Statskonsultnotat 2000-7.

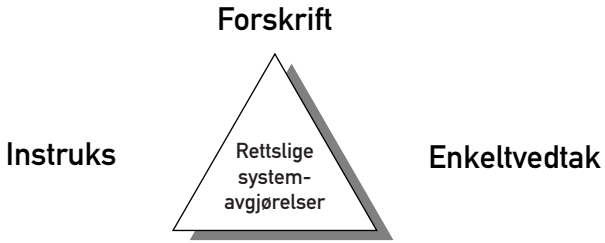
Torstein Eckhoff og Eivind Smith, konkludert med at det vanskelig kan tenkes at rettslige systemavgjørelser kan ses som forskrifter. Jeg kommer ikke nærmere inn på begrunnelsen for dette, men viser til drøftelsen i Schartum (1989). Samtidig er det imidlertid grunn til å understreke at denne konklusjonen ikke innebærer at det ikke kan og bør stilles krav som *ligner* de krav som stilles ved utarbeidelse av forskrifter. Begrunnelsen er i så fall ikke etterlevelse av forvaltningslovens bestemmelser, men ivaretagelse av grunnleggende forvaltningsrettslige prinsipper om forsvarlig saksbehandling.

De rettslige systemavgjørelsene som inngår i utviklingen av beslutningssystemer ligner også på fastlegging av instrukser og retningslinjer for rettsanvendelse og saksbehandling. Likevel er det noen vesentlige forskjeller som gjør at systemavgjørelsene ikke kan ses på som instrukser:

- Rettslige systemavgjørelser kan ofte ikke sies å være rettet mot saksbehandlere. Dette er i alle fall sant i tilfelle der automatiseringsnivået er høyt og det ikke forutsettes at en saksbehandler (i særlig grad) skal foreta selvstendige vurderinger av den maskinelle behandlingen. Når beslutningssystemene har en høy automatiseringsgrad må det rettslige innholdet i dem i utgangspunktet sies å være *direkte* rettet mot en ubestemt krets av personer, lignende det som gjelder for forskrifter.
- I forhold til tradisjonelle instrukser vil rettslige systemavgjørelser normalt kreve langt større dekningsgrad og større grad av systematisk tilnærming i forholdet til de aktuelle rettsspørsmålene. Mens en i tradisjonelle instrukser kan tillate seg å velge ut rettsspørsmål som i praksis har vist seg å skape spesielle problemer, samt spørsmål som det fra sentrale myndigheter har vært spesielt viktig å sikre styringen av, må rettslige systemavgjørelser treffes systematisk og uttømmende innenfor de aktuelle saksområdene. Dette innebærer at det må gis anvisning på løsningen av så vel enkle som vanskelige spørsmål.
- Mens tradisjonelle instrukser kan variere med hensyn til hvor bydende innholdet er, og således klassifiseres som alt fra klare direktiver til retningslinjer og anbefalinger, vil rettslige systemavgjørelser i utgangspunktet framstå som avgjørelser som alltid skal følges (av maskinen). Dette kan riktignok modifiseres av eksplisitte unntak i tradisjonelle instrukser som gjelder bruken av beslutningssystemet, f eks slik at det på bestemte punkter instrueres om at det skal skje en rimelighetsvurdering av resultatet fra den maskinelle rutinen, eller ved at de maskinelle rutinene ikke er utformet slik at de gir et endelig resultat. I utgangspunktet er det likevel hensiktsmessig å se de rettslige systemavgjørelsene som avgjørelser som uten avvik fastsetter hva som er de korrekte rettslige løsningene av de spørsmål som systemavgjørelsene omfatter.

- Rettslige systemavgjørelser nedfelles gjerne dels i form av spesifikasjoner til programmerer, dels direkte som programkode og dels som dokumentasjon. Min alminnelige erfaring er at de beskrivelser som gjør bruk av naturlig språk (spesifikasjon og dokumentasjon) ofte er ufullstendige som kilde til kunnskap om hva de rettslige systemavgjørelsene går ut på. En vanlig forskjell mellom tradisjonelle instrukser og rettslige systemavgjørelser er med andre ord at det ofte er vanskeligere å tilegne seg detaljert kunnskap om innholdet av rettslige systemavgjørelser enn i innholdet av tradisjonelle instrukser.

Etter min mening *kan* ikke rettslige systemavgjørelser klassifiseres som forskrifter og bør ikke klassifiseres som instrukser. Selv om slike beslutninger langt på vei kan sies å determinere resultatet i enkeltsaker, kan en åpenbart heller ikke klassifisere de rettslige systemavgjørelsene som «enkeltvedtak». Rettslige systemavgjørelser er snarere resultatet av en egen type rettslig beslutningsprosess. Denne beslutningsprosessen kan sies å ligge mellom to tradisjonelle typer beslutninger som forvaltningsorganer har kompetanse til å treffe; nemlig instrukser om rettsanvendelse og saksbehandling på den ene side, og enkeltvedtak på den annen. Samtidig har den trekk som ligger nær utferdigelse av forskrifter.



Rettslige systemavgjørelser bør betraktes som en egen type rettslig beslutningsprosess som ligger mellom tradisjonelle beslutningstyper, og som derfor ikke direkte er regulert eller omfattet av tradisjonell teori.

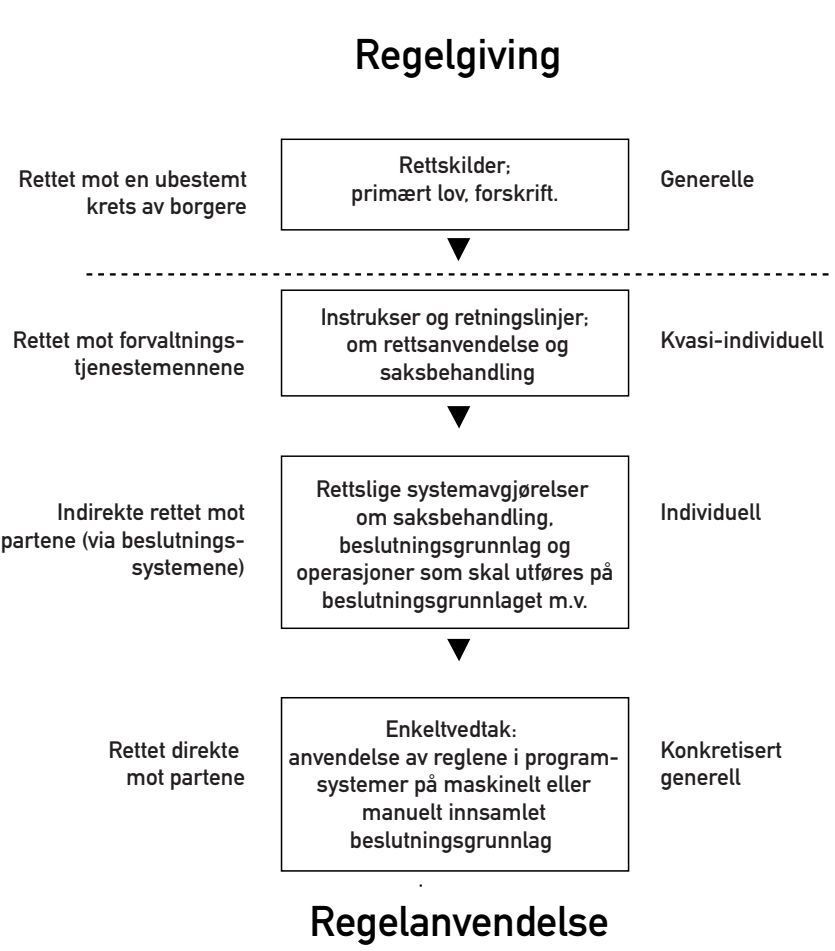
Den nevnte konklusjonen betyr i utgangspunktet at læren om forvaltningens instruksjonsmyndighet og ligningslovens bestemmelser om enkeltsaksbehandling mv ikke uten videre kan legges til grunn når kravene til de rettslige systemavgjørelsene skal formuleres. Resultatet er heller ikke at rettslige systemavgjørelser kan/vil måtte treffes i et «rettstomt rom»: I stedet må slike avgjørelser treffes ut i fra prinsippet om forsvarlig saksbehandling. Dette

innebærer bl a at en med utgangspunkt i dette prinsippet bør vurdere analogisk anvendelse av elementer fra læren om instruksjonsmyndighet, regler for enkeltsaksbehandling og regler for behandling av forskrifter. Jo mer rettslige systemavgjørelser kan sies å være lik en av de nevnte avgjørelsestypene, jo større grunn er det til å vurdere analogisk anvendelse.

Denne rettslige plasseringen av de rettslige systemavgjørelsene gir åpenbart en krevende arbeidssituasjon for skatteetaten (og alle andre etater som har ansvaret for utvikling av beslutningssystemer). Kort sagt ligger hovedproblemet i at rettslige systemavgjørelser er resultatet av en type rettslig beslutningsprosess som det ikke finnes noen allmenne saksbehandlingsregler for, og der det heller ikke finnes noe godt etablert rettsteori.

Den overordnede forpliktelsen for forvaltningsorganer er å sørge for at deres myndighetsutøvelse blir forsvarlig, uansett hvorledes de ulike deler av denne myndighetsutøvelsen klassifiseres eller organiseres. Enkeltvedtak fra en automatisert beslutningsprosess er resultatet av en serie der minst tre forskjellige rettslige beslutningsprosesser inngår, og som henholdsvis resulterer i beslutningstypene instruks, rettslig systemavgjørelse og enkeltvedtak.

Jo høyere automatiseringsgraden er, jo viktigere blir de rettslige systemavgjørelsene. Samtidig reduseres betydningen av den individuelt rettede enkeltsaksbehandlingen, det vil si den delen av saksbehandlingen som skjer ut i fra en forståelse av de konkrete forhold i hver enkelt sak. Enkeltvedtaket er imidlertid ikke bare resultatet av individuell rettsanvendelse, men av samspillet mellom generell, kvasi-individuell og individuell rettsanvendelse. Saksbehandlingen skjer med andre ord over tre nivåer: Det første nivået innebærer en detaljert generell forståelse/fortolkning av lover, forskrifter og andre rettskilder i form av (tradisjonelle) instrukser. Det andre nivået innebærer ytterligere detaljering og fortolkning i form av kravspesifisering og programmering (rettslige systemavgjørelser). Dette leddet innebærer en detaljering/fortolkning i så stor grad som det er mulig/nødvendig i forhold til den maskinelle behandlingen. Detaljeringsgraden er slik at det ofte vil foreligge løsninger av «alle» tolkningsspørsmål som kan forekomme innenfor vedkommende sakstype. Fordi alle kan finne løsningene på «sitt problem», kan dette nivået sies å framstå som «kvasi-individuelt». Det tredje nivået er den konkrete anvendelsen/kjøringen av programmene, der de generelle og detaljerte løsningene på rettsspørsmålene anvendes på enkeltsaker og kuliminerer med formelle enkeltvedtak. Er automatiseringsgraden høy, vil denne delen av saksbehandlingen kunne framstå som forholdsvis nøytrale driftsoppgaver, se avsnitt 8 (nedenfor).



Det er med andre ord tale om en sammenhengende kjede av myndighetsutøvelse som spenner fra det generelle og lite spesifiserte til det individuelle og detaljerte. Det er også forskjeller med hensyn til hvem myndighetsutøvelsen er rettet mot og hvorledes dette skjer. I de delene av myndighetsutøvelsen som ligger til forvaltningsorganene (under den stiplede linjen på figuren) må hver del være i tråd med kravet til forsvarlig saksbehandling.

Saksbehandlingsregler og rettsteori er tradisjonelle og viktige eksempler på virkemidler som anvendes for å etterleve kravet om forsvarlig saksbehandling. I mangel av regler og teori er forvaltningen avhengig av å løse oppgaven konkret. Utfordringen ligger da primært i å forholde seg til de rettsspørsmål som

er knyttet til de rettslige systemavgjørelsene og sammenhengen mellom disse avgjørelsene samt andre mer tradisjonelle avgjørelsestyper.

Manglende evne til å forstå og løse de rettsspørsmålene som er knyttet til systemutviklingen vil etter min vurdering være avgjørende for muligheten av å endre på arbeidsdelingen knyttet til systemutvikling og drift av beslutningssystemer, se nedenfor avsnittene 5–8. Årsaken er kort sagt at det ansvarlige forvaltningsorganets styringsevne kan bli utilstrekkelig i forhold til de styringskrav som følger av prinsippet om forsvarlig saksbehandling. Slike problemer kan imidlertid (langt på vei) avhjelpes ved å utforme generelle saksbehandlingsregler og -rutiner for utvikling av beslutningssystemer i etaten, se den videre framstillingen.

2 Om adgangen til å delegere offentlig myndighet

For å forstå hvor grensene går for hva og på hvilke måter et forvaltningsorgan kan sette bort arbeidsoppgaver til andre private aktører (eventuelt til sideordnede offentlige etater), er det etter min mening avgjørende å klargjøre grensene mellom kompetansetildeling i form av delegasjon og endret arbeidsdeling uten at myndighetsforholdene endres. Jeg tar ikke opp spørsmålet om delegasjon i sin fulle bredde, men avgrenser til spørsmål jeg mener belyser hovedproblemstillingen vedrørende eksternalisering («outsourcing») av arbeidsoppgaver vedrørende IT-funksjonen til private.

Delegasjon betegner overføring av et forvaltningsorgans kompetanse til å treffe offentligrettslige avgjørelser til et annet forvaltningsorgan eller til en privat organisasjon (mv) på en slik måte at den tildelegerte aktøren får samme kompetanse som det forvaltningsorganet som delegerer. Delegasjonsadgangen er uttrykk for forvaltningens organisasjonsmyndighet, og forutsetter normalt at den aktør det delegeres til er underlagt instruksjonsmyndighet. I det følgende forutsetter jeg «egentlig delegasjon», det vil si en situasjon der kompetansen til å treffe avgjørelser gis til en annen organisatorisk enhet enn den som har primærkompetansen.

Uansett hvilken avgjørelsesmyndighet det er tale om å delegere, er vilkåret for at det kan sies å foreligge delegasjon at *avgjørelsen treffes av* en annen enn den myndighet som innehar vedkommende primærkompetanse. Dersom det er saksforberedende funksjoner eller andre støttefunksjoner som et forvaltningsorgan ønsker å sette bort til andre, er det med andre ord ikke tale om delegasjon. I så fall er det bl a ulovfestede prinsipper om forsvarlig saksbehandling som avgjør i hvilken grad slik endret arbeidsdeling er lovlig eller ikke (og ikke rettsteori om delegasjonsadgangen).

Det må understrekes at spørsmålet om hvem som kan treffe avgjørelse i en sak ikke er av formell karakter, men forutsetter en konkret vurdering. Dersom

et saksforberedende arbeid som utføres av private leder ut i resultater som uten videre legges til grunn av den forvaltningsmyndighet som formelt treffer avgjørelsen, vil den saksforberedende aktøren reellt sett måtte ses på som beslutningsfatter. I så fall må kravene til lovlig delegasjon være oppfylt, jf nedenfor.

Når delegasjonsadgangen skal vurderes er det nødvendig å skille mellom Regjeringens og departementenes delegasjonsadgang på den ene side og på den andre side underordnede forvaltningsorganers adgang til å delegere. For den først nevnte gruppen er det i forvaltningsrettslig teori antatt at det i utgangspunktet er en forholdsvis vid adgang til å delegere både forskrifts- og enkeltvedtakskompetanse, og at slik delegasjon også kan tenkes til et sideordnet organ eller til et privat selskap eller organisasjon. Det er likevel ikke tilfellet at slik delegasjon kan skje uansett, og spørsmålet avhenger av en konkret vurdering av relevante lovbestemmelser, formålet med loven, reelle hensyn mv.

For delegasjon fra underordnede organer er det klare utgangspunktet motsatt: Det er ikke adgang til delegasjon av myndigheten til å treffe forskrifts- eller enkeltvedtak uten at det er klare holdepunkter for dette i lov. I slike tilfelle kan det med andre ord ikke delegeres til et side- eller underordnet forvaltningsorgan eller til en privat organisasjon eller et privat selskap.

Når delegasjonsadgangen i følge rettsteorien er stengt i forhold til kompetansen til å treffe forskrifts- og enkeltvedtak, er det etter min mening en sikker konklusjon at det samme i utgangspunktet også må gjelde for kompetanse til å treffe rettslige systemavgjørelser.

Konklusjonen er med andre ord at et underordnet forvaltningsorgan ikke kan delegere kompetansen til å treffe rettslige systemavgjørelser til sideordnede forvaltningsorganer eller til et privat selskap eller lignende uten at det foreligger klar hjemmel for dette i lov. For Finansdepartementet er utgangspunktet motsatt, dvs det er mulig at en etter en konkret vurdering vil kunne konkludere med at departementet kan delegere sin myndighet til sideordnede organer eller til private.

Jeg kommer ikke her inn på spørsmålet om hva som eventuelt skal til for at vilkårene for delegasjon fra departementet til (f eks) et privat firma. Årsaken er at jeg anser muligheten for en positiv konklusjon å være meget liten. Det er her nok å nevne at den aktuelle kompetansen er av inngripende karakter (fastsette beregningsgrunnlag, beregne skatter med videre) og at delegasjonen må være særdeles omfattende for at et privat selskap skal kunne settes i stand til å treffe de rettslige systemavgjørelser som er nødvendige for å utvikle og videreutvikle et helhetlig beslutningssystem.

Det er dessuten et poeng at det neppe er noen grunn til å velge delegasjon til et privat selskap eller til en sideordnet myndighet. Slik jeg har forstått behovet for å eksternalisere arbeidsoppgaver som har tilknytning til beslutningssystemene, gjelder det først og fremst å endre *arbeidsdelingen* ved bl a å

sette bort deler av utvikling og drift til en organisasjon utenfor skatteetaten. Jeg har på den annen side forstått det slik at det *ikke* er behov for å endre på *myndighetsforholdene*. I så fall er de avgjørende spørsmålene:

1. Hva som er den «nedre grensen» for delegasjon?
2. Hvilke krav må stilles til utførelsen av oppdrag som en privat organisasjon utfører for skatteetaten og som har nær tilknytning til etatens myndighetsutøvelse?

3 Den «nedre grensen» for delegasjon og krav til myndighetsutøvelsen i tilknytning til eksternalisering av saksforberedelse og drift

Ovenfor har jeg presisert at det ikke er tale om delegasjon med mindre det skjer en kompetansetildeling og endring av myndighetsforhold. Spørsmålet er så hvilke funksjoner som må utføres av et forvaltningsorgan for at vi skal kunne si at organet har avgjørelsesmyndigheten i behold? Etter min mening er de fire følgende kravene retningsgivende for vurderingen:

- Forvaltningsorganet må på informert grunnlag reellt avgjøre alle spørsmål om rettsanvendelse.
- Forvaltningsorganet må på informert grunnlag reellt avgjøre alle spørsmål om skjønnsutøvelse.
- Forvaltningsorganet må på informert grunnlag avgjøre hvorledes saksforberedende funksjoner som utføres av en privat aktør eller lignende skal være for å tilfredsstille krav til forsvarlig saksbehandling.
- Forvaltningsorganet må på informert grunnlag avgjøre hvorledes driftsfunksjoner som utføres av en privat aktør skal være for å tilfredsstille krav til forsvarlig saksbehandling.

Forvaltningsorganet må på informert grunnlag reellt avgjøre alle spørsmål om rettsanvendelse.

I dette kravet ligger det at det er forvaltningsorganet som må angi 1) hvilke rettsspørsmål som det er nødvendig å ta stilling til og 2) hva som er en rettsriktig løsning av disse rettsspørsmålene. Innenfor denne rammen må private aktører kunne brukes i vid utstrekning, f eks i forbindelse med framfinning av underlagsmateriale, analyse, programmering, testing mv.

Forvaltningens myndighetsutøvelse vil i praksis primært være knyttet til utarbeidelse av rettslige relevante deler av kravspesifikasjonen, dvs de deler av

spesifikasjonen der det er gitt anvisning på hvilke rettsspørsmål som skal håndteres av beslutningssystemet og hva disse løsningene består i. Det er sjelden mulig å spesifisere på en måte som fullt ut lar seg realisere uten at programmerer eller andre finner grunn til å foreslå løsninger som på bestemte punkter avviker fra den opprinnelige spesifikasjonen. Kravet til forvaltningsorganets kontroll med rettsspørsmålene innebærer derfor at forvaltningen også skal avgjøre spørsmål om endring og avvik fra den opprinnelige spesifikasjonen. For de rettslige spørsmålene skal det mao være et 1:1 forhold mellom spesifikasjonen/dokumentasjonen og det som faktisk er nedfelt i beslutningssystemet/programkoden. Uten et slikt 1:1 forhold vil det i realiteten ha skjedd en faktisk (og dermed ulovlig) delegasjon av offentlig myndighet. Enkelte sentrale forhold vedrørende rettsanvendelsen knyttet til utvikling av beslutningssystemer er behandlet nedenfor i avsnittene 4 og 5.

Forvaltningsorganet må på informert grunnlag reellt avgjøre alle spørsmål om skjønnsutøvelse.

Dette spørsmålet gjelder tilfeller der regelverket gir anvisning på en avveining som ikke er av (en ren) rettslig karakter, f eks dersom forvaltningsmyndigheten er gitt kompetanse til å avgjøre hva som skal anses å være «nødvendig», «rimelig», «forsvarlig» eller lignende. Kravene til forvaltningsmyndighetens kontroll med slike spørsmål tilsvarer trolig de krav som ovenfor er beskrevet for rettsspørsmålene. I forholdet til representasjon i datamaskinprogrammer mv innebærer dette bl a at det må være forvaltningsorganet som tar stilling til om skjønnsspørsmål skal håndteres innenfor de maskinelle rutinene eller ikke, og på hvilken måte dette eventuelt skal skje. Her som for rettsspørsmålene er det den løsningen som faktisk er realisert i systemet som myndigheten skal ha godkjent. Enkelte sentrale forhold vedrørende skjønnsutøvelsen er behandlet nedenfor i avsnitt 6.

Forvaltningsorganet må på informert grunnlag avgjøre hvorledes saksforberedende funksjoner som utføres av en privat aktør eller lignende skal være for å tilfredsstille krav til forsvarlig saksbehandling.

Forvaltningsorganet må i vid utstrekning kunne la private foreta saksforberedende oppgaver, også slik at private aktører forestår den rettslige informasjonssøking og de analyser som legges til grunn for forvaltningens beslutninger vedrørende rettsanvendelse og skjønnsutøvelse (jf ovenfor). For at en slik arbeidsdeling kan anses å være forsvarlig må det imidlertid trolig kreves at forvaltningsorganet stiller systematiske og bindende krav til hvorledes den private aktøren skal utføre oppgavene. Således vil det ofte være aktuelt å stille krav til formell kompetanse, undersøkelsesmetode og

dokumentasjon av utført arbeid. Jo større betydning det har at kvaliteten av det arbeidet den private aktøren utfører er høy, jo mer detaljert og streng må trolig forvaltningens krav til arbeidets utførelse være. Innen forvaltningsområdet skatt og avgift må kravene jevnt over forventes å være høye.

Forvaltningsorganet må på informert grunnlag avgjøre hvorledes driftsfunksjoner som utføres av en privat aktør skal være for å tilfredsstille krav til forsvarlig saksbehandling.

Drift av beslutningssystemer kan ikke uten videre sammenlignes med andre driftsoppgaver, bl a fordi drift i denne sammenhengen innebærer at en medvirker til at den rettsanvendelse som er foreskrevet i programmene faktisk utføres til den tid som er fastlagt. Det må derfor også stilles krav fra forvaltningsmyndigheten til private aktørers drift av ferdig utviklede beslutningssystemer. Kravene må omfatte spørsmål som sikring av krav til systemets konfidensialitet, tilgjengelighet og integritet (jf kap 9.1 om særskilte krav etter personopplysningsloven). Dette innebærer bl a at forvaltningsorganet må stille krav om tiltak mot uautorisert tilgang til systemet (opplysninger og programmer), uautoriserte endringer av opplysninger og programmer og tiltak for å sikre at systemet er tilgjengelig og i drift slik at krav til saksbehandlingstider og svarfrister med videre kan etterleves.

De kravene som jeg har nevnt ovenfor og som bør innfris for at saksbehandlingen kan sies å være forsvarlig, er ikke uttømmende. Det er dessuten et generelt poeng at kravene til forsvarlig saksbehandling både bør vurderes for hver av hovedkategoriene av spørsmål (jf ovenfor) og for myndighetsutøvelsen som sådan, dvs som en samlet vurdering.

4 Rettsanvendelsen knyttet til rettslige rammer for systemutvikling og -drift

Forvaltningsorganet må for det første avgjøre hva som utgjør det rettslige rammeverket for utvikling av beslutningssystemer og for driften av slike systemer. Rammeverket bør spenne fra det klart rettslige (lover, forskrifter mv) til dokumenter som har mer uklar rettslig status og med primært en internrettslig karakter (IT-plan og -strategi, serviceerklæring mv).

En privat oppdragsgiver kan selvsagt gjøre det saksforberedende arbeidet med kartlegging av aktuelle regelverk for forvaltningsorganet (jf avsnitt 7), men de aktuelle avgjørelsene skal treffes av forvaltningsorganet selv. Avgjørelsen av slike rettslige rammer bør herunder inneholde bestemmelser om betydningen av relevante rettslige reguleringer for aktuell systemutvikling eller -drift. For eksempel bør det fastlegges hvilken betydning anskaffelsesregelver-

ket har for kjøp av konsulenttjenester i et utviklingsprosjekt eller for kjøp av driftstjenester.

Forvaltningens avgjørelser vedrørende det rettslige rammeverket bør spesielt gjelde forholdet mellom ulike rettslige reguleringer der det kan sies å være konflikt. Arkivloven og personopplysningsloven utgjør f eks begge rammer for deler av utviklingsarbeidet og for driftsforhold, f eks fordi begge lover regulerer spørsmål om lagring av opplysninger. I flere situasjoner oppstår det motstrid mellom bestemmelsene i de to lovene. Forvaltningsorganet kan i slike tilfelle ikke nøye seg med å avgjøre at begge lover får anvendelse, men må også gå inn og konkret angi hvorledes slik motstrid skal løses.

5 Rettsanvendelsen knyttet til transformering fra rettskilder til programkode

5.1 Hvilke problemer knyttet til systemutviklingen kan sies å være rettslige?

Det er vanskelig å etablere et skarpt skille mellom rettslige og ikke-rettslige spørsmål som gjelder transformering av rettskilder og derfor mellom rettslige systemavgjørelser og andre systemavgjørelser (f eks slike som kan sies å være av teknologisk karakter).

Det er neppe alltid fruktbart å skille mellom rettslige *problemer* og rettslige *konsekvenser*: Omtrent alle livsforhold kan tenkes å ha rettslige konsekvenser, uten at vi dermed ser på de forhold som kan produsere slike konsekvenser som rettslige. Et beslutningssystem kan f eks rammes av systemteknisk svikt, noe som igjen kan foranledige erstatnings- og straffeansvar osv. Teknologiske, praktiske og andre forhold som kan gi rettslige konsekvenser er derfor i utgangspunktet ikke rettslige i seg selv. Likevel bør også slike spørsmål ses som rettslige dersom det i bindende rettsregler eller i rettsavgjørelser er stilt bestemte rettslige krav til hvorledes teknologien skal anvendes, til hvorledes de praktiske forholdene skal legges til rette mv. I vår sammenheng må dette betraktes som rettslige rammevilkår for systemutviklingen, se forrige avsnitt.

Dersom vi spesielt skal vurdere hvilke rettsspørsmål som aktualiseres i tilknytning til transformeringen fra rettskilder til programkode, er det mer hensiktsmessig å si at rettslige problemer foreligger *når løsningen av et problem krever anvendelse av juridisk metode*. I utgangspunktet bør forvaltningsorganet treffe avgjørelse i alle spørsmål som er av en slik art. Ved utvikling av beslutningssystemer oppstår de fleste og vanskeligste spørsmålene vedrørende rettsanvendelse i tilknytning til transformeringen av rettskilder (primært lover og forskrifter) i naturlig språk til datamaskinprogrammer.

Den rettsanvendelsen som er knyttet til transformering av rettskilder til programkode, innebærer kort sagt at rettskildene tolkes og at dette tolkningsresultatet uttrykkes ved hjelp av et programmeringsspråk. Slik fortolkning og transformering spenner over alle vanskelighetsgrader fra det elementære til den avanserte rettskildebruk og juridisk argumentasjon. I den ene enden av skalaen er tilfeller der transformeringen skjer ved at et formelt uttrykk i en forskrift eller lignende (f eks en tabell) overføres til et annet formelt uttrykk (program) uten at det egentlig er behov for noen kvalifisert juridisk innsats. I den andre enden av skalaen er rettsspørsmål som krever utstrakt gjennomgang av rettskildemateriale og skarpskodd anvendelse av juridisk metode. Jo større juridisk vanskelighetsgrad og tolkningsrom, jo viktigere er det at det er forvaltningsmyndigheten som treffer avgjørelsen.

5.2 Avgrensing av IT-systemet og fastlegging av automatiseringsnivå

Et helt sentralt rettslig (prosessuelt) spørsmål som forvaltningsorganet må ta stilling til er hvorledes avgrensingen av den IT-baserte delen av det samlede informasjonssystemet skal være, dvs spørsmålet om hvilke deler av rettsanvendelsen som skal automatiseres og hvilke deler som skal utføres manuelt. Slike valg vil være av avgjørende betydning for spørsmålet om saksbehandlingskvalitet og må derfor anses å være en sentral del av etatens myndighetsutøvelse.

Til spørsmålet om IT-systemets avgrensing hører blant annet flere spørsmål vedrørende hvorledes beslutningsgrunnlaget i enkeltsakene skal innhentes. I den utstrekning beslutningsgrunnlaget hentes maskinelt fra eksterne kilder blir dette også et spørsmål om grenseflaten mellom IT-systemer hos andre forvaltningsorganer, oppgavepliktige mv.

I tillegg til å ta stilling til hvilke kilder som skal benyttes for innhenting av beslutningsgrunnlaget i enkeltsaker, på hvilken måte innhenting skal skje mv, er det en sentral oppgave for forvaltningsorganet å ta stilling til hvilket omfang det skal være på den maskinelle behandlingen. Selv om all den prøving av vilkår og alle de beregningsoperasjoner som regelverket gir anvisning på kan gjøres til gjenstand for programmering, kan det i konkrete tilfellet likevel være at det ikke er rettslig forsvarlig å legge opp til automatisert behandling. Dette gjelder ikke bare tilfeller der regelverket forutsetter utøvelse av skjønn (jf avsnitt 6). I enkelte tilfeller vil rettskildene f eks kreve at det skjer en helhetsvurdering av saker som kan sies å ligge i en rettslig gråsone. I tillegg vil det kunne være økonomiske eller administrative årsaker til at en avstår fra å automatisere deler av saksbehandlingen, f eks fordi et regelverk forventes opphevet eller fordi regelverket er for komplisert og regulerer et for lite antall saker til at det er regningssvarende å transformere det.

Den mest omfattende oppgaven som gjelder den rettsanvendelse som vedrører transformering av rettskilder, er å ta stilling til tolkningsvalg. Ordlyden

i lov, forskrift og rettskildene for øvrig vil ofte gi grunnlag for flere mulige fortolkninger. Forvaltningsorganet må avgjøre hvilken fortolkning som skal nedfelles i beslutningssystemet. Slike avgjørelser må i det minste gjelde alle tolkningsspørsmål som ikke tidligere er avgjort i instruks eller lignende, alle tolkningsspørsmål der tradisjonelle instrukser ikke gir entydig svar, samt alle tolkningsspørsmål som tidligere er avgjort i instruks på en måte som avviker fra den løsning som ønskes valgt for beslutningssystemet.

Arbeidet med transformering av rettskilder vil ofte avdekke mangler ved det gjeldende regelverk og øvrig rettskildemateriale. Det kan f eks oppstå behov for å supplere eksisterende regelverk med helt nye bestemmelser eller la eksisterende regler få videre anvendelse enn det som direkte følger av bestemmelsen selv. Alle slike tillegg må avgjøres av forvaltningsorganet.

6 Spesielt om skjønnsutøvelse og rettsanvendelse av vage kriterier

Myndighetsutøvelsen i enkeltsaker kan dels bestå av rettsanvendelse (jf ovenfor) og dels skjønnsutøvelse. Skjønnsutøvelsen forutsetter langt på vei en åpen vurdering som i det enkelte tilfellet kan vise seg å bli kompleks, og som derfor ofte vil framstå som vanskelig. Rettsanvendelsen kan dels sies å gjelde enkle tolkningsspørsmål («faste kriterier»)[2] og dels vanskelige tolkningsspørsmål («vage kriterier»). Selv om så vel utøvelse av forvaltningsskjønn som rettsanvendelse i forhold til vage kriterier kan være vanskelige, er de forskjellige bl a fordi vurderingene styres av ulike normer. Mens rettsanvendelsen styres av juridisk metode, styres forvaltningsskjønnet av faglige og/eller fagpolitiske vurderinger (innenfor en rettslig ramme). I begge tilfeller kreves det imidlertid en vurdering og et resultat som framstår som korrekt og forsvarlig i forhold til den enkelte sak. Både rettsanvendelsesspørsmålet om en person «forsørger barn under 18 år» og skjønnsspørsmålet om det foreligger et «faglig forsvarlig helsetilbud» forutsetter individuell vurdering. I de fleste tilfeller vil det imidlertid ikke foreligge reell tvil, og avgjørelsen vil derfor framstå som kurant. I begge tilfeller vil det imidlertid lett kunne forekomme vanskelige tilfeller som krever inngående undersøkelse og vurdering.

Enten en velger å predefinere i de maskinelle rutinene hvilke kilder som skal nyttes for å innhente skjønnsmessige og/eller vage opplysninger, eller en velger å la en saksbehandler ta stilling til slike spørsmål i hvert enkelt tilfelle,

2 Eksempler på slike faste kriterier er alder, kjønn, sivil status, stilling mv. Også forhold som refererer til formelle avgjørelser, kan stilles i samme kategori, f eks «ilignet inntektsskatt siste år» eller «utbetalt lån i Statens lånekasse for utdanning». I de fleste saker kan slike opplysninger innhentes maskinelt, uten at det oppstår uenighet mht hva som er riktig faktum.

må disse rutinene tilfredsstille kravene til forsvarlig saksbehandling. Etter min mening kan en ikke hevde at skjønnsavgjørelser ikke kan undergis automatisert behandling i mindre utstrekning enn avgjørelse av vage kriterier. På samme måte som det kan være mulig å erstatte kriteriet «forsørger barn under 18 år» med en kombinasjon av opplysninger fra barnetrygdregisteret, folkeregisteret mv, vil det kunne være mulig å erstatte «faglig forsvarlig helsetilbud» med opplysninger om godkjente helsetilbud, lister over autorisert helsepersonell eller lignende. I begge tilfeller kan en på forhånd vite at det vil være enkelttilfeller som tilfredsstiller kriteriet, men som faller utenfor i de maskinelle rutinene. I begge tilfeller vil det derfor være behov for rutiner/tiltak som supplerer den maskinelle rutinen.

Det er mulig at det regelmessig vil være flere tilfeller som faller utenfor kriterier som er ment å erstatte skjønnsutøvelsen, men det kan i utgangspunktet neppe være avgjørende for hvor akseptable de maskinelle løsningene er. Poenget er mao at det *uansett* er problematisk å erstatte konkrete vurderinger av vage og skjønnsmessige kriterier med maskinelle rutiner. Spørsmålet om slike rutiner likevel må anses å ligge innenfor kravet til forsvarlig saksbehandling må avgjøres ut i fra hvor treffsikker rutinen er, hvor alvorlige konsekvensene av feil er, hvilke rutiner som er etablert for å fange opp tilfeller som faller innenfor kriteriet men utenfor den maskinelle rutinen og så videre. Etter min mening kan en mao ikke i utgangspunktet hevde at anvisning på skjønnsutøvelse i loven forutsetter at et menneske vurderer hvert enkelt tilfelle. For at dette skal være tilfellet må en etter min mening kreve klare holdepunkter i lov, forskrift, forarbeider eller annen autorativ rettskilde.

Konklusjonen er at det må være forvaltningsorganet som treffer avgjørelsen både vedrørende skjønnsutøvelse og rettsanvendelse (enten det er tale om faste eller vage kriterier). Forvaltningen må antas å ha en stor grad av valgfrihet med hensyn til om de ønsker å ta stilling til slike spørsmål som del av en manuell enkeltsaksbehandling eller som en del av utformingen av beslutningssystemet og de maskinelle rutinene. Uansett valg må myndighetsutøvelsen vurderes på bakgrunn av kravet til forsvarlig saksbehandling. Det er grunn til å tro at det gjennomgående vil være mer krevende å innfri slike krav dersom en velger maskinelle hovedrutiner for håndtering av vanskelige avgjørelser av skjønn og vaghet.

7 Krav til saksforberedelse mv

Kravet om at skatteetaten må sikre kvaliteten i det saksforberedende arbeidet hos en privat oppdragstaker gjelder både i forhold til rettsanvendelse og skjønnsutøvelse. Dette innebærer for det første at forvaltningsorganet må sikre en viss balanse i saksutredningsarbeidet, og at arbeidet blir gjort med til-

strekkelig grundighet. Det er neppe tilstrekkelig at en fastsetter at saksutredningen skal være «så god som mulig» eller lignende. Trolig må det kreves at forvaltningsorganet stiller opp spesifikke krav til hvorledes den private oppdragstakeren skal arbeide, f eks slik at det fastsettes kompetansekrav for de medarbeidere som skal utøve arbeidet, hvilke informasjonskilder som skal nyttes, hvilke kontrollrutiner den private aktøren selv skal følge mv. I tillegg må det fastsettes hvilke kontrollrutiner som forvaltningsorganet skal kunne utøve vis a vis oppdragstaker, og en viss rett for forvaltningsorganet til å gi pålegg om endringer av oppdragstakers rutiner mv.

Det er ikke mulig generelt å angi hvilke elementer i et samlet krav til oppdragstakers saksforberedende arbeid som må på plass for at dette arbeidet kan sies å tilfredsstille kravene til forsvarlig saksbehandling. Her vil kravene åpenbart variere alt avhengig av hvor store og inngripende konsekvenser det vil ha for partene dersom saksbehandlingsarbeidet blir utført på en utilstrekkelig måte.

8 Spesielt om krav til drift

Jeg velger her å forstå kategorien «drift» som oppgaver uten rettslig betydning, dvs oppgaver som ikke er knyttet til saksforberedelse eller avgjørelse i spørsmål om rettsanvendelse og skjønnsutøvelse. Dette innebærer bl a at ethvert tillegg og alle endringer av rettslig betydning (jf rettsanvendelse og skjønnsutøvelse) av beslutningssystemet vil forutsette en rettslig systemavgjørelse, og faller derfor utenfor det som kan regnes til driftsoppgavene. På samme måte vil alle beslutninger om konkrete saksforhold i enkeltsaker falle utenfor, det vil typisk si manuell fastlegging av beslutningsgrunnlag.

Driftsoppgavene vil (derimot) omfatte det å faktisk kjøre/anvende de automatiserte beslutningsrutinene, både automatisk innhenting av beslutningsgrunnlag fra oppgavegivere med videre og den videre manipulering av disse opplysningene i beslutningssystemet. Årsaken til at det er forsvarlig å kategorisere dette som «drift», er at det ikke treffes rettslige beslutninger, men bare igangsettes predefinerte operasjoner. Avvik fra slike forhåndsdefinerte automatiserte rutiner som påvirker innholdet av enkeltvedtak, faller utenfor det som kan regnes til driftsoppgavene.

Selv om driftsoppgavene ikke er rettslige i den betydning at det ikke innebærer myndighetsutøvelse og ikke forutsetter juridisk metode for å utføre dem, kan måten disse oppgavene utføres på ha rettslige konsekvenser, jf ovenfor under avsnitt 5.1. Således kan lovbestemmelser med videre stille krav til hvorledes driftsoppgavene utføres, eller rettslige krav kan følge av alminnelige aktsomhetsnormer mv. Det er derfor avgjørende at forvaltnings-

myndigheten klargjør de rettslige kravene til driften av beslutningssystemene og fastsetter krav overfor oppdragstaker om gjennomføring av tiltak for å understøtte etterlevelse av kravene.

9 Særlig om ivaretagelse av personvern

Personopplysningsloven trådte i kraft 1 januar 2001 og er på flere måter relevant for de spørsmål som er diskutert i dette notatet. For det første inneholder loven nye krav til saksbehandling som også får anvendelse i ligningssaker, og som kan være aktuelle å implementere i beslutningssystemer. For det andre stiller loven krav til avtaleforholdet mellom en «behandlingsansvarlig» og en «databehandler» når oppgaven er å behandle personopplysninger. Forvaltningsorganet vil i denne sammenhengen være behandlingsansvarlige i forhold til den behandling av personopplysninger som skjer ved hjelp av beslutningssystemene, og eventuelle private oppdragstakere som påtar seg driftsoppgaver med videre vil være databehandler i lovens forstand. Det alt vesentlige av opplysninger som behandles i ligningssaker med videre er å regne som «personopplysninger», jf definisjonen i lovens § 2 nr 1.

Det følger av lovens §§ 13 og 14 at det skal utarbeides planlagte, systematiske og dokumenterte tiltak for å sikre personopplysningers konfidensialitet, tilgjengelighet og integritet, og for øvrig for å sikre gjennomføring av lovens bestemmelser, av forskrifter og eventuelle bestemmelser i konsesjoner og andre enkeltvedtak. I denne sammenhengen nøyer jeg meg med å peke på at denne dokumentasjonen skal være tilgjengelig for databehandlere, dvs oppdragstakere som driftsoppgaver mv er eksternaliserte til. Behandlingsansvarlige er ansvarlig for at databehandler etterlever sikkerhetstiltakene, og databehandlers plikt til dette skal kontraktsfestes (§ 15 annet ledd).

Viktigst i denne sammenheng er at databehandler/oppdragstaker ikke kan behandle opplysninger på annen måte enn det som følger av skriftlig avtale (§ 15 første ledd). Dette innebærer at alle de oppgaver som en oppdragstaker skal utføre for skatteetaten må være beskrevet i en skriftlig avtale. Det er uklart hvor detaljerte krav til beskrivelse som stilles opp, men det er på det rene at den ikke kan være av helt overflatisk karakter.

Etter personopplysningslovens § 24 kan innsynsrettigheter etter kap III i loven praktiseres ved henvendelse til databehandler (dvs oppdragstaker) for så vidt gjelder alle personopplysninger som databehandler behandler for skatteetaten, jf § 15. En slik rett overfor databehandler kan ikke avgrenses av avtale mellom skatteetaten og deres oppdragstakere.

10 Konklusjoner og avsluttende kommentarer

Jeg har i dette notatet bl a konkludert med at det i forholdsvis stort omfang kan gjøres endringer i organiseringen av skatteetatens IT-funksjon. Forutsetningen er at slike endringer ikke innebærer overføring av kompetanse til å utøve forvaltningsmyndighet. Endringer som innebærer overføring av forvaltningsmyndighet vil trolig måtte vurderes som ulovlig delegasjon til private.

Med forutsetningen om at det kun må skje en endring av arbeidsdeling og ikke av myndighetsforhold, har jeg undersøkt hvilke oppgaver som i utgangspunktet vil kunne tildeles private. Jeg har her pekt på at saksforberedende oppgaver (med hensyn til rettsanvendelse og/eller skjønnsutøvelse) og driftsoppgaver i utgangspunktet kan eksternaliseres.

En forutsetning for at eksternalisering av nevnte oppgaver kan skje, er at forvaltningsorganet selv treffer alle retts- og skjønnsavgjørelser. Jeg har videre forutsatt at denne avgjørelsesmyndigheten skal være reell, dvs at forvaltningen foretar en selvstendig vurdering av det beslutningsgrunnlag som framkommer ved hjelp av oppdragstakerens saksforeberedelser. Jeg har i tillegg forutsatt at forvaltningen stiller opp tilstrekkelige krav til det arbeidet oppdragstaker skal utføre (saksforberedelse og drift), slik at kravet til forsvarlig saksbehandling kan etterleves. Herunder har jeg pekt på at det i lovgivningen eksisterer krav vedrørende driften med videre, noe jeg har illustrert ved å trekke fram enkelte bestemmelser i personopplysningsloven.

Jeg har også konkludert med at det i utgangspunktet ikke er noen grunn til å avvise at skjønnsavgjørelser kan erstattes av automatiserte rutiner, idet jeg legger til grunn at forvaltningen uansett må tilfredsstille krav til forsvarlig saksbehandling. Det er etter min mening ingen grunn til å sette skjønnsavgjørelser i en egen kategori i så måte. Samtidig er det på det rene at det ikke er trivielt å ha automatiserte rutiner som trer i stedet for en individuell vurdering av skjønnsmessige og vage vurderingstemaer.

Avslutningsvis vil jeg peke på at eksternalisering av oppgaver til private ikke innebærer at kravet til skatteetatens styring av de aktuelle oppgavene minsker. Den største forskjellen i forhold til å utføre oppgavene i eget hus er trolig at styringen i stor grad må skje ved hjelp av kontrakter og ikke ved hjelp av generelle og individuelle instrukser til de medarbeidere som skal utføre oppgavene. Det er grunn til å anta at kontraktsstyring vil være mer krevende enn styring ved hjelp av instruksjonsmyndighet. Samtidig er en omfattende kontraktsregulering en forutsetning for eksternalisering. Dersom eksternalisering gjennomføres på lovlig og forsvarlig måte, antar jeg derfor at den reelle styringen av saksutredning i tilknytning til systemutvikling og drift av systemene kan bli tettere enn det den i dag er under den vanlige instruksjonsmyndigheten.

Litteratur

Bing (1977): «Automatiseringsvennlig lovgivning», *Tidsskrift for rettsvitenskap* 1977 s 195–229.

Eckhoff/Smith (1999): *Forvaltningsrett*, 6 utgave, Tano-Aschehoug 1999.

Schartum (1989): «Om den offentlige forvaltningens edb-programmer, deres rettslige innhold og stilling som forskrift», *Tidsskrift for rettsvitenskap* 1989 s 650–677.

Schartum (1993): *Systemutvikling og rettssikkerhet i offentlig forvaltning*, Universitetsforlaget 1993.

Rynning (1976): «En fremstilling og vurdering av reglene for tildeling av bostøtte», *Skriftserien Jus & edb* nr 17, Institutt for privatrett, Avdeling for edb-spørsmål, Oslo 1976.

Crossing the Schengen external border

STEPHEN K KARANJA

1 Introduction

As part of my study on control of persons in Europe, I decided to cross the borders between Austria and her two non-Schengen neighbours, Hungary and Slovakia, in March 2001. I chose these particular borders because I would experience control from two perspectives: the Schengen border control by the Austrian authorities and the traditional border control by the Hungarian and Slovakian authorities. The objective was to investigate the effectiveness of the Schengen Information System in border control by comparing it with the traditional border control in Hungary and Slovakia.

2 Crossing the Austrian-Hungarian border

It was a Saturday morning on 3.3.2001 when I boarded the *Vienna – Budapest Keleti* train from the*Westbahnhof* in Vienna. Perhaps because it was a Saturday there were not many people travelling that morning. Consequently, I was able to occupy one compartment of six seats all alone. Many passengers, especially those travelling alone, seemed to do the same. Those travelling in a group of six or less were also able to occupy a single compartment too as a group.

The train departed on schedule at 8:25 am. We passed through the residential and commercial suburbs of Vienna. Just a short distance from the city of Vienna, the suburbs gave way to farmlands. During this time of the year it is the winter season; the farmlands were bare and the trees looked dry and dead having shed their leaves the autumn before. The scenery was not at all attractive as the weather was cloudy and grey with a downpour threatening and the landscape monotonously flat. At such a time, travellers often take refuge in their reading materials. I resisted the urge to bury myself in a book I had brought along and instead kept staring at the unattractive landscape the monotony of which was occasionally broken by villages and scattered buildings as we cruised along. I did not know exactly what I hoped to see but I kept on looking. I presume that because this was my first time along this route I did not want to miss anything of interest.

The first interruption to my silent observation of the landscape came from the train ticket inspector who requested to see my ticket. I gave it to him, he stamped it and then left with a word of "danke" to continue routine ticket checks with other passengers.

A short distance again and we arrived at a little railway station and if it were not for a sign proclaiming "Willkommen in Bruckreudorf Burgenland", it would have passed unnoticed just as another railway station. In fact, this was a border station but there were no border control guards or any other physical objects to indicate we were now crossing the Schengen external border and entering Hungary.

A short while later as the train took off again, two uniformed border control officers came. They were young, dressed in dark blue service uniforms, with Gendarmerie-looking caps. The first entered into my compartment while the other remained outside in the corridor. The one in my compartment demanded to see my passport, which I obligingly handed to him. He first examined the opening page bearing my personal details, then he threw a quick inquisitive look at me and back at the passport again. He perused the pages of the passport and then spoke to his colleague. When the other responded, the first officer called out the number of my passport and I could see the other officer enter the information on a laptop computer. After a short while, the officer murmured something to the first officer who, without hesitation, handed back the passport to me with a word of "danke". This was apparently the end of the Schengen external border control by the Austrian border authorities. As I experienced it, the control was quick, impersonal and non-confrontational. The seemingly magical Schengen Information System had apparently exclaimed that I was "clean". The negative hit had apparently cleared me and confirmed that I was a desirable person. For Schengen purposes, I was now free to proceed with my journey to Budapest. However, in the back of my mind, I was wondering what would have happened if the hit were positive; ie, if the system were mercilessly to have declared that I was not "clean", that I was an undesirable person.

Before I could find an answer to this question, two men entered the compartment. They wore full military fatigues with pistols dangling from their trouser belts. One did not need to be told who they were; these were obviously Hungarian control authorities. The manner in which they were dressed, together with their body language, reminded one that not so long ago Hungary had been a communist state. Both men looked mean and at the same time surprised to see a black man seated in a compartment by himself. Their looks – particularly those of the first man to enter the compartment – were also mischievous; the men seemed to proclaim victory over their prey even before they had announced the nature of their business. When the first man

thought it was time for business, he curtly demanded to see my passport. As he read the information on the passport cover, I saw his expression take on a cunning, salivating smile. I knew at once that this guy meant only trouble. Yet I remained calm as I knew that there was no fault with my document – after all, the Schengen Information System had declared me "desirable".

The man opened the personal information page and read every entry carefully. Then he stared at the photograph and cast a long doubtful look at me. He turned back to the photograph and back to me again. The seesaw action continued for some minutes. Eventually he stopped the game. He then began perusing the rest of the passport page by page, minutely reading every piece of information inserted there. If nothing was inserted, he stared at the blank page as if expecting it to magically reveal what he was looking for. After reaching the end of the document, he removed a reading lamp from his pocket, turned it on and, with its purple luminescent light, scanned every page of the passport. He repeatedly scanned the personal information page. Thereafter, he moved to the corridor and, with the natural light of the sun, scrutinised the personal information page over and over again. Failing to get what he was looking for, he turned back to me and asked if I had any other identification document with me. I replied I had none. He inquired whether I had a driving license with me. I replied I hadn't. This seemed to confirm his suspicion. However, I volunteered that I had a bankcard with similar details as in the passport. He quickly dismissed the idea but still demanded to see the card. I handed it to him but it did not seem to strike any positive impression on him. After casually looking at it, he handed it back to me. I then volunteered that I had a letter from the University of Vienna which could help alleviate his doubts. I handed the letter to him but he did not bother looking at it. Either he could not read the German language in which the letter was written or he did not like the idea that my identity could be true. His apparent preconception was that my identity was false and that my supporting documentation could only be fake. However, there was no way he could prove this. He eventually accepted the inevitable, stamped my passport with an entry visa, then hurriedly left the compartment. It was now the turn for his colleague who until now had not uttered a word to state his business.

As if to declare that he was a customs official, the second officer asked me for my luggage. I pointed to my small rucksack. He demanded to know whether that was all the luggage I had. I said that it was. He then asked how many days I was going to stay in Budapest. I replied that it was only one day. He asked whether I had any money with me. I said yes and he demanded to see it. I showed him the 7,000 florints I had. He asked whether that was all. I replied that I had credit cards too. He asked to see them. I showed them to him and he looked satisfied and left.

After this unpleasant ordeal, I tried to sit back and catch up with what I had missed outside. Pleasantly, when I looked outside the window, the dull flat landscape had given way on the left side of the train to a contrasting range of hills covered with patches of snow. To the right, the same flat landscape continued but was now made attractive by a thin layer of snow covering the ground. This change of landscape was soothing; I was able to relax somewhat and forget the distressing incidents a few minutes ago. However, as I settled down into a restive mood and anticipation of Budapest, the first Hungarian officer accompanied by two others, a man and woman, all dressed in military uniform, entered into the compartment. From the looks on their faces, I could tell this mission did not look good at all.

The new man demanded to see my passport. I handed it to him but this time, determined to continue with my own thoughts, I decided to try to ignore them as they carried out their business. Yet they were not going to let this be. The man asked me whether I was born in Kenya, a very unnecessary question as the document he was staring at stated so. Without looking at him, I replied yes. He continued and asked me how long I intended to stay in Budapest. I replied, still looking out the window, one day. He then quipped cynically, "tourist!". I casually replied yes. He then asked if I had another identity document, but the first officer seemed to tell him that I didn't. However, I replied that I didn't. As he did not speak to me again, I decided to check what they were now doing and saw him scanning the passport, page by page, with the same purple illuminating lamp. As he reached the end of the document, he did not seem to know what to do next, so he started shaking it vigorously as if expecting some of the pages to fly off. This did not happen. Then with frustration marked all over their faces, they consulted together, perhaps about the next course of action. Thereafter, I saw the woman reach out for a piece of paper and start scribbling details from my passport. Afterwards, she handed me the paper and asked me to write down my details. What she had written down was "Etternavn", "Fornavn", "Fødselsdato" and "Utstedt den"; ie, Norwegian formulations for surname, given names, date of birth and place of issue. I filled in the information and handed the paper back to her. After this, they seemed to give up for a short while. Then the woman asked me to sign the paper. I signed it and then when she compared the signature with the one in the passport, she conferred with the others and they all seemed to accept defeat. She handed the passport back to me and they hurriedly left.

The rest of the trip continued without interruption except for the Hungarian ticket inspector who came in, inspected my ticket and then left. We were now approaching Budapest. It was raining outside, promising a wet Saturday in Budapest.

After a relatively relaxing and interesting time in the city – during which I on several occasions was helped by hospitable Hungarians to find directions, etc – it was time to catch the last train of the day back to Vienna. Again, with the kind help of local people, I was able to find my way to the central railway station, Budapest-Kileti, for the return trip. I did not want my memories of Hungary to be spoiled by the work of overzealous border control authorities. I bought a bottle of *Tokaji*, the Hungarian trademark white wine, as a pleasant addition to the hospitality of a great country and people.

The trip back to Vienna was initially filled with the good memories of Budapest. Even the lack of lights in my compartment seemed to go well with the need for relaxation. So I decided to doze off as the journey started. The only interruption was from the Hungarian train conductor who came in briefly and left after his business. But halfway into the journey, I was awakened by the entry of the Hungarian border control authorities. This time, a young man and an elderly woman, each dressed in military uniforms, demanded to see my passport. As I handed it to them, I could sense, even with the darkness in the compartment, their disbelief and doubts. Another ordeal was about to unfold.

The young man perused each page of my passport using a spotlight he was carrying. Then he came back to the personal details page and scrutinised the photograph before rudely casting the beam of light in my face. He did this continuously for more than a minute. Thereafer, he directed the light to the passport again and then back again to my face. He seemed to be in even greater doubt now, or so he made it look, because the photograph was only two years old. I thought that I could not have changed that much to create such difficulties of identification. But he seemed determined to have it his own way. He took out the now trade-mark purple illuminating lamp and started to scan page after page of the passport. When he came to the end, he looked more frustrated than ever before. Then, as if to say he was not short of tricks, he removed another light from his pocket and placed one end to his right eye. It was reminiscent of one of the instruments that doctors use to check ears or the one used by watch repairers to examine tiny parts of the watch or jewel dealers to establish authenticity of stones. With his gadget, he scanned again the passport page by page. Whatever he was looking for was not there but he was not ready to give up.

He resorted to another trick. He removed a piece of paper from his bag and gave it to me. He demanded I fill in the required details. I told him I could not do this in darkness. It then occurred to him that I needed light to carry out his command. He illuminated with his spotlight as I filled in the details. However, in the middle of the exercise he changed his mind and told me that they needed to carry out more controls on my passport and that I should therefore accompany them to their office. I obliged and took my coat and bag,

but as we moved on, they kept up with the control of other passengers and I had to stop and wait while they carried out their work. Eventually, the train stopped at a railway station and the young man asked me to alight. This is when I realised that they did not have an office in the train and we had to leave the train to an office at the station. I disembarked and the young man followed behind. Just outside the platform we met an elderly officer and the young man started to explain to him the problem with my passport. The officer asked me if I had a credit card. I said yes and gave him my bankcard, the same card I had given to the control officer in the morning. The bankcard bore my photograph and similar personal details as my passport. The officer compared the two documents and concluded that there was no problem of identity. He stamped my passport and returned it to me apologising for the misunderstanding. He then asked me to return to the train and wished me a safe journey. I sighed with relief. At long last there was a reasonable man in the Hungarian border control squad; a man who did not let his prejudices taint his judgement and sense of duty and who was able to accept that a black man can have a valid foreign European passport.

Back in the train, the Austrian Schengen border controllers came. One entered my compartment and asked for my passport. I gave it to him and after perusing it he gave my name to a second officer who had a laptop computer. Again, my name and passport were checked against the Schengen information database. The laptop officer mumbled something and the other one handed me the passport and they were gone. Again the Schengen control was fast and without confrontation.

A short while later, the train conductor came and asked us to leave our wagon as it was going to be detached from the rest of the train due to the lighting problem. We moved into the other lighted wagons and the journey began again. The Austrian ticket controller came and performed his ritual. I was then left alone to enjoy the rest of the journey, which continued without incidents. Soon we reached Vienna *Westbahnhof*. I left the train and headed for the underground subway line 3 to the city centre and later walked to the comfort of my room at *Benedictushaus, Schottenstift* to begin writing on my border control experience before the details faded in my memory.

What conclusions can one reach from this experience? First and foremost, the Schengen system has made the work of decision making for its officers easy and efficient. Decisions are based on facts and less on intuition. There is either a hit or no hit. Secondly, the Schengen system makes controls less burdensome for the travellers. There are no searching questions or confrontation if your identity is in order. The identity is established quickly. The Schengen system works splendidly well for someone who "has nothing to hide" or rather if the system declares such. Of course, even with the Schengen system,

there is room for prejudices. For example, a person of "black origin" will more often than not have his/her passport checked against the system.

On the other hand, the Hungarian officers seemed to be motivated by prejudices. They also seemed to have very little faith, if any, in their own control mechanisms and instruments. Perhaps they were also suffering from an inferiority complex for lack of a modern and efficient system like their Schengen counterpart. They stubbornly wanted, therefore, to establish that their methods are still the most effective by proving the Schengen system wrong.

However, another important lesson one can learn from this episode is the effect of Schengen/EU border control measures and policies on "non-European" / "non-white" citizens with European national passports or foreign nationals with resident permits for a European country when travelling in third countries. It is not uncommon for third countries' authorities to carry out severe and confrontational controls on such persons due to the pressure exacted on these countries by Schengen/EU countries. The Schengen/EU States have imposed the task of checking the genuineness of these persons' passports on these countries, a task that the latter are poorly equipped to handle. For example, in January this year, while travelling from Kenya back to Norway, the airline staff were required to check the genuineness of my passport and of all other "non-white" travellers using a European national passport. The airline staff did not have a secure way of doing this. They resorted to taking photocopies of the passports of those concerned. They also demanded – like the Hungarian officials – for additional proof of identity, such as identity cards. I also know of a case where one traveller was refused to board the aircraft because the airline officials suspected his passport not to be genuine. The matter was resolved when the person got a letter from the embassy concerned in Nairobi the following day. The controls are creating unnecessary difficulties (bordering on discrimination) for these travellers. The problem lies with poor, inaccurate control procedures based on suspicion.

3 Crossing the Austrian – Slovakian border

After the encounter at the Austrian-Hungarian border, it was time to experience the controls at the border between Austria and Slovakia. On 7.3.2001, I took the 10:15 am train from Vienna's *Südbahnhof* bound for Bratislava. As we headed north-eastwards, we passed through the Viennese suburbs. These soon gave way to farmlands on both sides of the rail line. The landscape was flat as far as the eyes could see. There was bright sunshine and some early signs of spring in the farmland. The day promised to be beautiful and interesting. Staring outside was a relaxing experience. The only pall was a layer of light blue smog in the air.

The journey proceeded without any notable incidents except for the appearance of the Austrian ticket inspector who quickly performed his duty then left. The train was quite empty; most of the travellers occupied compartments of six seats alone. The distance between Vienna and Bratislava is about 64 kilometres and expected to take approximately one hour. With the good weather and beautiful landscape, the journey seemed even shorter as we approached Bratislava. The train made its second stop at a railway station on the outskirts of Bratislava. The station looked empty with unfinished but modern constructions. Some passengers alighted here and since there was no visible sign to indicate which station this was, I decided to go into the corridor and ask. The man who was near me could not speak English but a woman at the far end of the corridor came to my aid and explained in fairly good English that we were at Bratislava. However, she added that if I wanted to go to the city centre, I should alight at the next station, which was the last one. I thanked her and went back to my compartment and waited for departure.

While sitting there lost in my thoughts, the first of the border control authorities came. This was an Austrian gentleman wearing a dark blue uniform with the inscriptions of the Gendarmerie and a pistol dangling on the side of his right hip. He requested to see my passport. I handed it to him. He looked thoroughly at the personal details page but only casually at some of the other pages. He then handed it back to me. This time, no inquiry was made against the Schengen system. I thought this was a mistake and perhaps that a second round of control was to come.

True, a second round did eventuate but this time it was the Slovakian authorities who were in charge. Again, only one person came, a young though tall and heavily built lady. She wore a green jacket with an emblem, American khaki trousers and a green cap bearing an emblem also. She did not carry a weapon. She pleasantly asked to see my passport. I handed it to her and she keyed the passport number into a hand machine she was carrying. She then perused, rather quickly, the passport pages. Near the end of the passport she put a visa stamp. She then handed the passport back to me and departed. This left me with a mixed feeling. Something did not seem to be right; I still expected to see officers again. But they did not come.

Soon afterwards, the train started moving and we crossed a huge bridge over the mighty Danube. The train meandered through the suburbs, which bore traces of hard times. A few new high-rise buildings and the castles of Bratislava could be seen from the distance. The impression I got was of an old city which had been neglected but is now getting a facelift. Eventually, we entered the railway station. I left the train, proceeded to a tourist information office where I bought a city map, then entered the old part of the city by foot.

My day in Bratislava was interesting and went by quickly. It was soon time to get back to the railway station to catch my return train. I got lost several times when trying to find the station. Fortunately, the local people were hospitable and ready to help; the only handicap was that very few could speak English. However, in their determination to help, an understanding was always reached and I was able finally to reach the railway station. Checking the train departure timetable board, though, I could not locate my train. I decided to enquire at the information office. When the lady at the counter checked my ticket, she informed me that my train was departing from another railway station! Panic almost hit me but the attendant came to my rescue and gave me instructions on how to get there by taking a particular bus. When I embarked on the bus, I was told that I could not buy a ticket inside the bus. The driver tried to explain to me where the automatic ticket machine was but I could not risk going out and being left behind. I had only 34 minutes before my train departed. The bus drove through the busy streets of the city with numerous stops and I feared I would not make the train. But we reached the railway station with ten minutes to departure time.

Here, though, I could not find my way to the platform from where the train was departing. Again, I had to avail myself of the hospitality of my Slovakian hosts. Fortunately, the man I turned to could speak English very well and he informed me that I first had to pass through immigration controls. He was kind enough to accompany me to the door leading there. The first desk one came to belonged to the Slovakian border authorities. The lady behind the desk looked casually at my passport and then handed it back to me requesting that I proceed to the next desk. This was the Schengen control counter. Two officers sat behind it. I handed my passport to the first one who looked at it and then gave it to the other officer sitting with a laptop computer. He keyed passport information into the computer, then talked to his colleague who handed me back the passport. I asked them where the platform was and they kindly pointed out the platform and the train. I got into the train and one or two minutes afterwards I was underway to Vienna.

The exhaustion of the last hours had really taken a toll. As soon as I made myself comfortable in the seat, I dozed off. The Slovakian ticket inspector had to wake me up to inspect my ticket. As soon as he was gone, I continued with my sleep which was later interrupted by the Austrian ticket inspector. After he left, I was now fully awake and began to enjoy the scenery outside. The landscape looked more beautiful this time with the impending sunset. Vienna's *Südbahnhof* was not far away and as soon as we reached there, I took a tram to my hotel room to relax and write this report when the details were still fresh in my mind.

Again, the Schengen border control proved to be quick, targeted, without confrontation and less cumbersome. The same principle seemed to apply: "if you have nothing to hide", or rather, if the system declares this to be so, "you have nothing to fear". The system also seemed to aid the officer in reaching a decision quickly and conclusively. The Slovakian authorities seemed sure and confident in their control system. They did not display indecision like the Hungarians. The Slovakians too did not seem to operate with the same degree of prejudice; their judgement, therefore, was not blurred. However, one could observe that they might not have been keen on their border control for other reasons. For example, they seemed to trust the Schengen control system. If the Schengen control did not reveal anything wrong, then there was nothing to worry about. In addition, since Slovakia is not in the first round of countries to join the EU soon, they may display a slack attitude towards border control.

Online aftaler i USA[1]

HENRIK SPANG-HANSSEN

1 Indledning

Online aftaler er praktiske fordi de på sekunder muliggør online handel og ofte indeholder de forum klausuler og forsøger dermed at løse spørgsmål om stedligt værneting.[2] Sådanne aftaler vil uden tvivl blive særdeles almindelige i fremtiden verden over i forbindelse med brug af Internet, og første spørgsmål vil derfor for en domstol i en stor andel sager blive om den pågældende online aftales forum klausul er gyldig i domstolens forum. Mange online aftaler indeholder tillige vilkår om voldgift, som ligeledes kan være grundlag for at en domstol må afvise en sag, hvortil bemærkes, at US Supreme Court gentagne gange har talt til fordel for brug og godkendelse af voldgiftsaftaler.[3]

Det kan i den anledning være værdifuldt at se på erfaringer fra USA, der indtil 1999 omfattede mere end 50 % af al handel på Internettet, og hvori der fra perioden 1995 er afsagt en hel del domme om online aftaler. I denne forbindelse bør bemærkes, at USA med undtagelse af staten Louisiana er et »common law« land, og domstolene er således også lovgivere, hvorfor der nedenfor tillige vil blive redegjort for regler, som kan udledes fra diverse domstolsafgørelser.

Der findes i USA kun et fåtal af egentlige lovregler om online aftaler. Det næstfølgende vil kort gennemgå visse regelværker, som i visse retsafgørelser har været anvendt til støtte for rettens argumentation.

---

1 Denne artikel er delvis taget fra H Spang-Hanssen, *Cyberspace Jurisdiction in theUS*, CompLex 5/01 (Oslo, 2001), kap III.A.

2 Det er værd at bemærke, at selv efter mere end 10 års retspraksis har ingen domstol i USA fundet grundlag for at kunne anvende de generelle værnetingsregler, men har i hvert enkelt tilfælde nøje undersøgt om en websides indhold kunne hjemle anvendelse af en ekstraordinær værnetingsbestemmelse. Se fx sagen *Westcode, Inc v RBE Electronic, Inc*, 2000 WL 124566 (ED Pa 2000).

3 Også i Canada er online aftaler blevet godkendt, se *Rudder v Microsoft* [1999] Carswell–Ont 3195 (Ontario Superior Court, Oct 1999).

2 Typer af aftaler

Aftaler oprettet ved brug af computere har i USA været givet mange navne såsom »click-wrap«, »click-through«, »web-wrap«, »browse-wrap« og »access-contracts«. Betegnelsen »mass-market licenses« har Uniform Computer Information Transactions Act (UCITA) reserveret til en speciel type af visse standard forbruger transaktioner, jf. § 102. De gennem retspraksis udformede regelsæt for disse computergenererede aftaler er forskellig fra aftaler, som har været indeholdt i fysiske pakninger, og som i USA er betegnet som »shrink-wrap«, »break-the-seal«, »blister-pack«, »wrap-around«, »box-top«, »in-the-box« eller »tear-me-open«.

På det sidste er der i USA for så vidt angår aftaler indgået ved brug af computere – og oftest online – sket en differentiering af regelsættende mellem »browse-wrap« og andre typer af »click-wrap« online aftaler. Karakteristisk for online aftaler er, at vilkår eller brugerbetingelser normalt er tilgængelige gennem en link nederst på første websiden, og at der oftest kræves klik på en YES-knap eller et ikon på skærmen, skrivning af »I Agree« eller lignende for at få adgang til yderligere websider, en funktion eller et program. Nogle har betegnet den sidste type »web-agreements« og defineret sådanne som en af to typer: (a) aftaler som indebærer at køberen eller brugeren må rulle gennem vilkårene og skrive »I Agree« for derefter at klikke på et ikon som eksekverer godkendelse; (b) vilkår som kræver at køberen eller brugeren klikker på et »accept« ikon hvorefter accept straks transmitteres til modparten.

Den største fordel ved computergenerede aftaler er, at der undgås bevismæssig tvivl om afgivet accept af vilkår og dermed grundlæggende krav for at gøre aftalen gældende. Men i praksis vil et retsligt krav om at brugeren altid skal klikke »I Agree« eller skrive navn og adresse for at give bevis for aftale om fx forumvalg og voldgift, skabe problemer for langt hovedparten af websideejere, idet adskillige undersøgelser har vist, at brugere undgår sådanne websider og i stedet hopper til andre sider. Brugere er generelt ikke villige til at give oplysninger om sig selv førend beslutning om køb og en større og større andel af brugere fravælger sider som kræver sending af »cookies«, hvorved modparten ikke har bevis for at en webside har været besøgt. Endvidere viser undersøgelser, at kun et fåtal af brugere ulejliger sig med at klikke på linken nederst på en webside for at undersøge vilkår for brug af websiden.[4]

4 Se fx ekspertudtalelse i *ACLU v Reno*, 31 F Supp 2d 473, 487 # 34-36 (ED Pa 1999).

3 Modellove og lovgivning

I USA har et halvoffentligt organ[5] udfærdiget flere modellove med henblik på Internettet. En af disse er UCITA af 1999. Modelloven er et resultat af 10 års arbejde og har til formål at skabe et regelsæt for computer informationsindustrien indeholdende udfyldningsregler for shrink-wrap licenser, online aftaler og garantiforpligtelser. Den anfører i § 5(b), at domstole bør undersøge indholdet og omstændighederne, herunder parternes adfærd for at afgøre om en køber eller en sælger har accepteret at indgå transaktioner.

At elektroniske aftaler tillægges stor betydning i USA og kun anses at kunne få reel værdi, hvis de er gældende over grænser, ses af, at den føderale regering i 2000 i al væsentlighed besluttede at ophøje modelloven Uniform Electronic Transactions Act (UETA) til en ufravigelig interstatslig lov, Electronic Signatures in Global and National Commerce (ESIGN).[6] Dette indebærer, at hidtidige føderale og statslige love, som fx diverse forbrugerbestemmelser i Californiens UETA-lov, skal tilsidesættes.

ESIGN gælder for de fleste transaktioner som relaterer sig til interstatslig eller udenlandsk handel. Den bestemmer, at hvor en lov kræver en skriftlig protokollering eller en underskrift er en elektronisk version lige så gyldig. Den hjemler endvidere specifikke forbruger beskyttelsesregler. Modsat UETA kræver ESIGN ikke at en person skal have accepteret brug af elektroniske optegnelser eller underskrift.

Modelloven UCITA, som indtil nu kun er lovfæstet af delstaterne Maryland og Virginia, indeholder deklaratoriske regler om »choice of forum« og »choice of law«, men er begrænset i relation til forbrugere, idet § 105(c) bestemmer, at hvis en handling og en betingelse i en kontrakt er i strid med en forbrugerbeskyttende regel, skal sidstnævnte gælde. For så vidt angår forumvalg hjemler UCITA i tilfælde, hvor der ikke er indgået en aftale om lovvalg, to udfyldningsregler:

(a) For en »access contract« eller en aftale som tilvejebringer elektronisk forsyning af en »copy« benyttes loven i den jurisdiktion, hvor licensgiver var lokaliseret, da aftalen blev indgået;[7]

5 National Conference of Commissioners on Uniform State Laws.

6 Electronic Signatures in Global and National Commerce, Chapter 96 of US Code, 15 USCA § 7001–7031 (2000).

7 Ifølge Official Comment 3: »The reason for this rule is that any other rule would require that the information provider comply with the law of all states and all countries since it may not be known or knowable where the contract is formed or the information sent. 'Located' does not depend on the location of the computer that contains the information«.

(b) I andre tilfælde er aftalen omfattet af loven i den jurisdiktion som har den mest signifikante relation til transaktionen.

UCITA § 110(b) angiver i relation til en aftalt klausul om forumvalg at en sådan kun er eksklusiv, såfremt (1) aftalen udtrykkelig tilkendegiver dette, (2) advis herom har været givet og (3) forumvalget ikke er urimeligt og uretfærdigt. Valg af et forum med tilknytning til en af parterne vil normalt være rimelig, og en sådan aftale vil normalt være at anse som retfærdig under hensyntagen til den risiko og usikkerhed som ellers ville eksistere.

Det skal være muligt at udskrive eller lagre aftalens vilkår, jf. §211. Ligeledes skal det være muligt forudgående at kunne gøre sig bekendt med aftalens vilkår og have valgmulighed for at kunne trække sig tilbage straks derefter og dermed undlade at indgå aftale, jf. §112. Ifølge den officielle kommentar til paragraffen skal vilkårene være tilgængelige på en måde som bør henlede en ræsonnabel person på adgangen til at gennemgå vilkårene. Vilkår er ikke tilgængelige for gennemsyn, hvis adgang til vilkårene er så tidsforbrugende eller præsentation er så obskur at gennemgang er besværlig. Vilkår, som er lettilgængelige gennem en elektronisk link, vil normalt opfylde kravene.

Disse hovedlinier fra ovenstående modellove synes at have lighed med adskillige domstolsafgørelser i USA.

Ved gennemgang af amerikanske domstolsafgørelser, især under det parallelle føderale domstolssystem, er det vitalt at se på de enkelte staters lovgivning, idet også de føderale domstolene skal anvende den lovgivning som er gældende for den stat, hvortil den føderale domstol er hjemmehørende. Dette bevirker, at især de føderale appeldomstole, som omfatter flere stater, må anvende forskellige staters sæt af fx forbrugerlovgivning.

Det er således af afgørende betydning for eksempel i relation til afgørelser fra Ninth Circuit at undersøge om sagen relaterer sig til fx delstaten Nevada, Washington, Alaska eller Californien, hvilken sidstnævnte har omfattende forbrugerlove, der for eksempel dels kræves, at en sælgers webside skal angive retur- og tilbagebetalingsret, dels giver forbud mod klausuler om forumvalg og lovvalg som hindrer forbrugere i at anlægge såkaldte »class actions«, hvilket sidstnævnte opfattes som et vitalt forbrugerankemiddel.[8]

8 Californian Business & Professions Code § 17538 (2000) og Californian Consumers Legal Remedies Act (Civil Code §§ 1750 *et seq*) og sagen *AOL v Superior Court County*, 2001 WL 695166 (Cal App 1 Dist, June 2001).

4 Retspraksis

I USA viser den langt overvejende retspraksis, at værnetingsklausuler, lovvalgsklausuler og voldgiftsklausuler godkendes også i forbrugersammenhæng. Den generelle holdning i USA er, at click-wrap vilkår er den eneste og rimelige tekniske mulighed som Internettet tilbyder. Trenden synes at være, at det er tilstrækkeligt for at en aftale er gyldig, at aftalen er tilgængelig for gennemgang forud for installering af software eller videre skridt fra en første webside, hvor vilkår kan læses ved en link nederst på websiden.

I sagen *ProCD*,[9] som ofte fejlagtigt har været anført som en shrink-wrap sag, anførte retten, at ProCd modsat mange andre sælgere ikke havde en skriftlig licens som blev effektiv så snart kunden rev pakningen op, men derimod blot anførte, at pakningen indehold software som indeholdt en licensaftale. Seventh Circuit fandt licensaftalen var gyldig, fordi »[the] software splashed the license on the screen and would not let the [user] proceed without indicating acceptance«. Retten bemærkede, at en bruger frit kunne vælge andet software, hvis han ikke kunne acceptere sælgers aftale, og at konkurrence mellem handlende – og ikke retslig gennemgang af en pakkes indhold – er måden kunder er beskyttet i en markedsøkonomi.

Domstole i USA har gentagne gange afvist et argument om at kunder er uden mulighed for at øve indflydelse på magtfulde sælgeres standardiserede aftaler, som indeholder valg af forum og lovvalg. Retten i *CompuServe*[10] opretholdt en sådan aftale og påpegede, at den handlende forlangte at kunden gentagne gange skrev »Agree« for dermed at bekræfte vilkår og konditioner, samt at aftalen udtrykkeligt angav at være indgået i delstaten Ohio – hvor sælger var hjemmehørende – og var »governed by and construed in accordance with [Ohio law]«.

I sagen *Caspi*[11] bemærkede retten, at en elektronisk kontrakt indgået med et klik på en mus er lige så bindende som en skriftlig kontrakt. Den afviste sagen i henhold til den handlendes påstand, da der var indgået en forum klausul om brug af den handlendes hjemting, og fordi retten hverken fandt, at click-wrap aftalen gav indtryk af at være resultatet af svindel eller særlig forhandlingsstyrke, at brug af forumvalget var i strid med statens politik, eller anvendelse af det valgte forum var uacceptabelt, uhensigtsmæssigt eller ville forhindre en rimelig retssag. Domstolen påpegede som mange andre, at brugeren frit kunne rulle gennem aftalevilkårene og påpegede, at accept-knappen – som skulle aktiveres for at komme videre – var placeret lige ved siden af rullevinduet med vilkårene, at der ikke var noget ekstraordinært ved størrelsen

9 *ProCD, Inc v Zeidenberg*, 86 F 3d 1447 (7th Cir 1996).
10 *CompuServe v Patterson*, 89 F 3d 1257 (6th Cir 1996).
11 *Caspi v Microsoft Network*, LLC, 323 N J Super 118 (N J Super Ct Add Div 1999), certification denied by *Caspi v Microsoft Network*, 162 N J 199 (N J 1999).

eller placeringen af forum klausulens tekst, at brugeren burde være klar over at have indgået en aftale, og at han havde muligheden for ikke at acceptere vilkårene.

Denne type for web-aftale betegnede domstolen i sagen *Specht*[12] som en »click-wrap,« modsat en »browse-wrap« licens, som tillader brugeren for eksempel at downloade og bruge software uden at kræve udtrykkelig og aktiv accept af vilkår. Dommen er udtryk for, at det ikke er uden betydning, hvor og hvorledes brugervilkår anføres på en webside, og synes at følge kravet i UCITA om, at aftaler ikke er gyldige, hvis tilgængeligheden for gennemsyn er så tidsforbrugende eller præsentation er så obskur at gennemgang er besværlig. På den anden side følger dommen ikke bemærkningen i UCITA om, at vilkår, der er lettilgængelige gennem en elektronisk link, bør anerkendes. Den handlendes webside indeholdt en farvetonet boks eller knap »Download« og ved at klikke herpå iværksattes nedlastning af et freeware. Retten påpegede, at websidens eneste reference til licensaftalen fremkom hvis brugeren rullede længere ned på skærmen, hvorefter følgende tekst blev synlig: »Please review and agree to the terms of the *Netscape SmartDownload software license agreement* before downloading and using the software«. Denne tekst anså retten ikke som et vilkår for brug af softwaren, men kun som en »invitation,« hvorfor et vilkår om voldgift ikke var gyldigt. Retten påpegede, at det primære formål med nedlastning er at skaffe en fil og ikke at indgå en aftale.

Fra amerikansk retspraksis kan endvidere nævnes, hvad der må betegnes noget nær det optimale for at sikre en licensaftales bindende virkning. Retten i *In re RealNetworks*[13] – også vedrørende freeware – godkendte klausuler om både forumvalg, lovvalg og voldgift i en omfattende aftale på utallige paragraffer, som var skiftevis i store og små typer og som skulle accepteres førend nedlastning kunne ske. Den påpegede, at aftalen var let udskrivelig og kunne lagres, hvorfor den var at anse som en »skriftlig« aftale, jf. ESIGN, og forefandtes på mere end en måde. En bruger kunne (a) med et højreklik på sin mus opmærke hele aftalen og kopiere den til ethvert skriveprogram og derefter udskrive den, eller (b) vælge at klikke på et særligt ikon for aftalen under menuen »Real« under »start-menuen«, fordi aftalen automatisk blev nedlastet til brugerens harddisk samtidig med softwarens nedlastning. Aftalen var derfor ikke utilgængelig eller uoverskuelig.

Domstolen fandt det uden betydning, at det aftalte forum var langt fra forbrugerens. Den fulgte den langt overvejende trend blandt amerikanske domstole, som sagen *Groff*[14] opsummerede til, at forbrugere ikke bliver tvun-

12 *Specht v Netscape Communications Corp*, 2001 WL 755396, F Supp 2d (SDNY, July 2001).
13 *In re RealNetworks Inc*, Privacy Litigation, 2000 WL 631341 (ND Ill May 11, 2000).
14 *Groff v AOL*, 1998 WL 307001 (RI Superior Court 1998). Anderledes *AOL v Superior Court County*, 2001 WL 695166 (Cal App 1 Dist June 2001).

get ind i aftaler, fordi der er konkurrence i online computer serviceindustrien og forbrugere dermed har valgmuligheder, at selvom den handlende har udformet aftalen, er modparten ikke under nogen form for forpligtelse til at acceptere vilkårene, fordi han blot kan afvise den handlendes ydelse, samt at det i den elektroniske alder ikke er helt klart, hvor en aftale er indgået, men at det er rimeligt at udpege dette til stedet, hvor den handlendes mainframe er lokaliseret.

I sidstnævnte relation bør bemærkes, at også EU Kommissionen har i flere sammenhænge tilkendegivet, at der i relation til Internet bør skiftes fra et forbrugersynspunkt til et sælgersynspunkt og dermed anvende den såkaldte »country of origin« regel. Men nogle amerikanske domstole har med relation til forbrugere stillet særlige krav og forlangt specielle funktioner på websider.

I *Stomp*[15] bemærkede den Californiske domstol, at ejeren af en webside med en interaktiv click-wrap aftale har muligheden for at begrænse, hvor ejeren kan blive sagsøgt, og at den sælger som ønsker at opnå fordelen ved ubegrænset interstatslig handel over Internettet, løber risikoen for at blive sagsøgt hvor som helst.

En domstol i Texas anførte i *American Eyewear,*[16] at online virksomheden kunne have undgået søgsmål i Texas ved for eksempel at tage skridt til at websiden indeholdt (a) en købsordre formular med en værnetingsbestemmelse, (b) en notits af ikke at ville sælge produkter til Texas, eller (c) en funktion som afviste godkendelse af ordre eller forsendelse til Texas hjemmehørende personer.

Men i praksis kan selv sådanne forsøg på at begrænse sig blive gjort illusoriske af domstole. I november 1999 oprettede en canadier i overensstemmelse med canadisk lovgivning en online tv-kanal, hvor brugerne på websiden for at kunne modtage tv-udsendelser forinden først skulle angive et canadisk postnummer og derefter erklære, at de befandt sig i Canada. Desuagtet afsagde en amerikansk domstol ordre om, at websiden skulle fjernes, da den ikke fandtes at udelukke amerikanere fra at skaffe sig adgang til webside, fordi disse blot kunne opgive falsk canadisk postnummer og erklæring.[17] Begrundelsen giver anledning til overvejelser om, hvilke undtagelser, der i den elektroniske verden, vil blive udfundet af domstole mod gyldigheden af elektroniske aftaler, som ellers af lovgivere er givet samme værdi som en skriftlig, jf f eks ESIGN.

På det seneste er der udviklet adskilligt software til at lokalisere brugere, men dels indebærer sådant software konflikt med adskillig personværnlovgiv-

15 *Stomp, Inc v NeatO*, LLC, 61 F Supp 2d 1074 (CD Cal 1999).
16 *American Eyewear, Inc v Peeper's Sunglasses and Accessories, Inc*, 106 F Supp 2d 895 (ND Tex 2000).
17 *20th Century Fox v iCraveTV*, 2000 US Dist Lexis 1013 (WD Pa, 2000).

ning, dels er funktionsdygtigheden under 80–90% og stærkt afhængig af hvilken access-provider brugeren anvender.[18] Retspolitisk må det findes betænkeligt at støtte sig på sådanne softwareløsninger, al den stund Internettets verdensbrugere i stadig hast finder løsninger og nye muligheder for at hindre funktionsdygtigheden af sådant sporingssoftware, ligesom den tekniske softwareudvikling sker så hurtigt og pludseligt, at hidtidigt software bliver forældet eller ikke fungerer med andet nyt software.

Nogle domme i USA er gået endog meget langt for at gennemføre lokale forbrugerbeskyttelsesbestemmelser. I *Granite Gate Resorts* [19] bestemte en domstol i Minnesota, som har en stærk forbrugerlovgivning, at indholdet på en webside om en påtænkt fremtidig virksomhed var tilstrækkelig tilknytning for at behandle sagen, selvom der ikke forelå bevis for, at der var indgået en eneste aftale med indbyggere i Minnesota. Websidens værnetingklausul blev tilsidesat, og retten fandt det uden betydning, at websiden indeholdt følgende notits: »Please consult your local, county, and state authorities regarding restrictions on off-shore sports betting via telephone before registering with Wagnernet«.

Den eneste tilknytning mellem Minnesota og virksomheden var, at websiden gav mulighed for, at personer kunne lade sig registrere på en mailingliste. I faktisk alle andre sager i USA har det været holdningen, at dersom en sagsøger ikke kan påvise, at der rent faktisk er indgået handler med indbyggere i domstolens forum hjemler de amerikanske værnetingregler ikke en domstol mulighed for at indkalde webside ejeren til møde i den pågældende domstol.

Det synes yderst foruroligende, at en vilkårlig domstol indkalder en udlænding på baggrund af en websides indhold og tilsidesætter en websides (forum-)vilkår, blot fordi disse er i strid med domstolens lovgivning og uden, at der foreligger noget bevis for, at der er handlet gennem websiden. Reelt set var eneste baggrund for sagen, at websiden – kald det annoncering – kunne ses også af den pågældende domstols borgere.

I relation til beskyttelsesregler for forbrugere på Internettet, hvortil brug af teknisk computer er nødvendig kan det overvejes om ikke brug heraf rettelig burde sammenlignes med de samme brugeres anvendelse af en teknisk automobil, hvorfor der i mange lande er objektivt ansvar eller omvendt bevisbyrde. Her bliver de som har anlagt veje, produceret trafiksignaler og biler kun i meget begrænset omfang inddraget i søgsmål på grund af brugerens automobilkørsel. Ligeledes kan overvejes, hvorfor en forbruger skal være mere beskyttet ved opkobling til et international netværk og adgang til køb

18 For eksempel vil medlemmer af America Online (AOL) blive registeret som hjemmehørende i Virginia, hvor AOLs hovedserver er placeret.

19 *State of Minnesota v Granite Gate Resorts, Inc*, 568 NW 2d 715, 720 and FN1 (Minn App 1997).

på udenlandske websider end når samme forbruger rejser til udlandet og dér køber samme ydelse, og hvor forbrugeren da er undergivet lovgivningen i sælgers værneting.

På den anden side er der ingen tvivl om at brugere af Internettet som alle andre steder skal have beskyttelse mod decideret svindel og bedrageri eller skjulte aftalevilkår,[20] men herom vil den normale sælger eller modpart være enig.

Forbrugere er nøjagtig så intelligente som de selv ønsker at være i situationen og de gør altid krav på at blive behandlet som uintelligente, når de har gjort noget galt.

Der synes i flere sammenhænge at ske en opblødning af den enkeltes forbrugerbeskyttelse til fordel for hensynet til flertallets menneskerettigheds hensyn, fx ytringsfrihed. Man må håbe, at den forbruger, som oftest ikke har problemer med at anvende selv de mest avancerede computerspil, tvinges til at lære, at ved at logge on til Internettet har den pågældende fjernet sig fra sit nærdemokratiske forbrugersikkerhedsnet og er som en turist taget til »udlandet«, hvor der højest sandsynligt gælder andre regler, som bør undersøges fremfor hæmningsløst at klikke sig rundt på websider uden at læse vilkårene for brug heraf. Dette vil indebære, at alle landes indbyggere – såvel sælgere og informationsgivere som købere og læsere – kan have ligeværdighed på internationale computernet, som dermed kan fungere som den homogene verdensomspændende enhed, som det er konstrueret til. Ellers, »if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning«.[21]

---

20 *Thompson v Handa-Lopez*, 998 F Supp 738 (WD Texas 1998).

21 E-mail af 24.11.2000 fra en af konstruktørne af Internettet, Vinton Cerf (også formand for Internet Corporation for Assigned Names and Numbers (ICANN) og tidligere professor ved Stanford Universitet) til Agence France-Presse i forbindelse med hans ekspertudtalelse til den franske domstol i sagen *La Ligue Contre le Racisme et L'Antisémitisme (LIGRA) v Yahoo!, Inc*, Tribunal De Grande Instance de Paris.

E-handelsdirektivet og elektronisk handel på tvers av europeiske landegrenser

PETER LENDA

1 Innledning

Bruken av Internett har de siste årene hatt en eksepsjonell vekst. Denne utviklingen har generert mange nye muligheter innen forretningslivet, og handel på nett – elektronisk handel – har fått økende oppmerksomhet. Den Europeiske Union (EU) ser på bruken av Internett som en unik mulighet for å knytte enda større kontakt mellom medlemsstatene og deres folk. Et av de viktigste initiativene for å fjerne mulige barrierer til denne utviklingen, er direktivet som koordinerer visse rettslige aspekter ved elektronisk handel (heretter kalt e-handelsdirektivet).[1]

Direktivet tar sikte på å øke handel mellom EU medlemstater ved å skape et minste sett med trygge, forutberegnelige kjøreregler for elektronisk handel. Direktivet er en type minimumsdirektiv som skal supplere eksisterende regler for slik handel. Direktivet må derfor sees i lys av de regler som allerede finnes, slik som Romakonvensjonen om lovvalg i kontrakt, fjernsalgsdirektivet, personverndirektivet, direktivet om elektroniske signaturer, direktivet om opphavsrett, forordningen om jurisdiksjon, osv.[2]

Artikkel 3 i direktivet stipulerer som hovedregel at den som tilbyr «informasjonssamfunnsstjenester» skal forholde seg til loven i det landet tilbyder er etablert. I forhold til interlegal rett, ligner bestemmelsen på en lovvalgsregel som ofte betegnes som «the country of origin rule», dvs at «senderlandets» eller «opprinnelseslandets» rett skal anvendes. Betydningen av en slik regel kan være stor avhengig av den teknologi som benyttes. Et eksempel på dette er nettområder («websites») som kan fungerer som «forretningslokaler». Hvis produktet (eller tjenesten) som selges er digitalt, kan nettområdet gjennom dets datamaskinprogram ta imot en bestilling og levere varen (eller tjenesten) uten at et menneske på selgersiden er involvert. Hvis et norsk firma som eier

1 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, 1).

2 Se videre avsnitt 3.2 nedenfor.

dette nettstedet plasserer det på en tjenermaskin i Portugal, kan det oppstå spørsmål om nettstedet da skal reguleres av norsk eller portugisisk rett.

Siktemålet med denne artikkelen er først og fremst å diskutere rekkevidden av art 3 og dermed rette søkelys på interlegale spørsmål som oppstår i forbindelse med implementering av e-handelsdirektivet. Artikkelen forsøker også å kast lys på sammenhengen mellom art 3 og EU-retten, først og fremst Romatraktaten.

2 Generelt om direktivet

Direktivets virkeområde er generelt begrenset til «information society services», dvs informasjonssamfunnstjenester. Dette begrepet – som finnes fra før, jf direktivene 98/48/EF og 98/84/EF[3] – dekker et stort antall tilfeller av økonomisk aktivitet som finner sted gjennom et telekommunikasjonsnettverk, slik som Internett. Den grunnleggende definisjonen av begrepet gjengis i fortalen til e-handelsdirektivet, punkt 17 (jf også punkt 18) som «any service normally provided for remuneration, at a distance, by means of electronic equipment…». Det som dekkes er både tjenester som leveres gratis og salg av varer og tjenester. Eksempler på dette er gratis e-mail tjenester, Internettilgang, søketjenester, Internettreklamer av forskjellige slag, salg av fysiske gjenstander, og salg av digitale produkter.[4] Aktivitet som skjer off-line, f eks fysisk levering av varer, dekkes derimot ikke av begrepet. Det samme gjelder for kringkasting i seg selv, eller kommunikasjon alene over Internett. Like viktig er at all ikke-økonomisk aktivitet på Internett faller utenom, slik som private hjemmesider og generell offentlig informasjon. Skillelinjene her vil imidlertid ofte være nokså diffuse i praksis.

Et annet vilkår ved informasjonssamfunnstjenester er at slike tjenester må foregå over distanse, altså at partene ikke er tilstede samtidig på samme sted. Dette betyr f eks at et dataspill som skjer on-line faller innenfor begrepets rekkevidde, mens et dataspill tilgjengelig i en spillehall faller utenfor.

Et tredje vilkår ved informasjonssamfunnstjenester er at de må skje med elektroniske midler med lagringskapasitet, slik at nedlasting av dataprogram-

3 Respektivt, Directive 98/34/EC of 22. june 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, 37), og Directive 98/84/EC of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access (OJ L 320, 28.11.1998, 54).

4 Med digitale produkter menes produkter som eksisterer i digital form og kan dermed overføres on-line. Digitale produkter kan være både tjenester og varer, eksempelvis en Internett–avis eller et datamaskinprogram. Enkelte digitale produkter er vanskelig å definere som enten varer eller tjenester, slik som musikk eller film i digital form som kan lastes ned til lagring eller til direkte avspilling («streaming»).

mer eller annen digital informasjon faller innenfor, mens salg av digital informasjon over en ekspedisjonsdisk på en lagringsenhet (f eks CD-ROM) faller utenfor. Her faller også reklame over faksimile eller Internettelefoni utenfor, siden disse skjer i «realtime» uten noen form for lagring. Den fysiske leveringen av varer som er bestilt på Internett faller også utenfor.

Til slutt må en informasjonssamfunnstjeneste skjer som respons til et individs spesielle forespørsel. Vanlig kringkasting faller dermed utenfor, men ikke f eks videosendinger på forespørsel («video-on-demand»). Et nettområde med informasjon om progammtilbudet til en tv-stasjon vil falle innenfor, men ikke den vanlige kringkastingen av tv-programmet.

Direktivet opererer med en rekke andre avgrensninger også. Skattespørsmål er f eks unntatt fra direktivets virkeområde (jf art 1 nr 5). Det samme gjelder personvernspørsmål som dekkes av direktivene 95/46/EF og 97/66/EF.[5]

3 Hovedregelen i art 3

3.1 Innledning

Hovedregelen i art 3 lyder:

> «1. Each Member State shall ensure that the Information Society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.
>
> 2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide Information Society services from another Member State».

Punkt 1 stipulerer at, i forhold til spørsmål som faller inn under det koordinerte området, skal en tilbyder av informasjonssamfunnstjenester følge de reglene i det landet tilbyderen er etablert i. Punkt 2 presiserer at hvis en tilbyder forholder seg til de aktuelle reglene, så kan ikke andre medlemsstater forhindre tilbyderen i å tilby sine tjenester i de andre medlemsstatene.

---

5 Respektivt, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, 31), og Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector (OJ L 24, 30.1.1998, 1).

Reglene representerer et ønske om at de enkelte medlemsstater ikke vil kunne forhindre at et selskap etablert i et medlemsland skal kunne bli hindret i å levere varer og tjenester til de andre medlemslandene. Dette gjelder spesielt små og mellomstore bedrifter som ofte ikke har midler til å ha faktisk representasjon andre steder enn der de er fysisk etablert. Et annet ønske er å skape forutberegnelighet for de enkelte aktører som investerer i e-handel (jf fortalen punkt 7).

I første omgang kan reglene virke enkelt og greit. De krever imidlertid en stor grad av presisering. For det første gjelder dette hva som ligger i at tilbyderen er etablert i et medlemsland – det må klargjøres hva som ligger i etableringskravet. For det andre må det presiseres hva som menes med det koordinerte området. I tillegg er det viktig å klargjøre sammenhengen mellom art 3 og EU-retten, kanskje først og fremst Romatraktaten. Til slutt må unntakene til hovedregelen (jf art 3 nr 3 og nr 4) klargjøres.

3.2 Sammenhengen mellom art 3 og EU-retten/Romatraktaten

Forholdet mellom art 3 og EU-retten generelt er sentralt. Allerede i fortalen til direktivet punkt 1, vektlegges forholdet til Romatraktaten art 14 nr 2 om fri flyt av varer og tjenester som et grunnleggende prinsipp bak direktivet. Prinsippet manifesteres bl a også i direktivet art 1 nr 1 som påpeker at direktivet er ment å bidra til at det indre marked fungerer.

Som en del av det EU/EØS-rettslige rammeverket skal direktivet være retningsgivende for visse spesielle forhold ved e-handel. Det skal samtidig være et supplement til og ikke erstatte eller forandre allerede eksisterende EU regler for informasjonssamfunnet (jf art 1 nr 3).[6]

Direktivets virkeområde begrenses videre av de rettsakter innenfor EU/EØS som er ment å etablere et minimumsnivå av beskyttelse for forbrukere og samfunnet ellers (jf art 1 nr 3). Det nevnes i denne sammenhengen regler for folkehelsen og forbrukervern spesielt, men det er klart at andre EU regler om minimumsvern også kan fungere som en skranke.

3.3 Sammenhengen mellom artikkel 3 og internasjonal privatrett

Det neste spørsmålet som må forfølges er sammenhengen mellom art 3 og interlegal rett. Det vil si, hvorvidt har art 3 aspekter av interlegal rett? Er den bare en gjennomføring av det indre marked?

Utgangspunktet i tradisjonell internasjonal privatrett vil etter min mening være at når private parter som ønsker å tilby eller kjøpe varer eller tjenester på Internett står overfor en lovregel som gir forventning om et valg av lov ved

6 Fortalen punkt 11 inneholder en skjematisk opplisting av disse reglene.

handel over landegrenser, representerer denne regelen en type lovvalgsregel etter internasjonal privatrett. Hensynet til forutberegnelighet er et viktig element bak et slikt argument.

Selv om dette hensynet taler for at art 3 representerer en type lovvalgsregel, må direktivet tolkes under ett. I direktivet art 1 nr 4 kommer det frem at direktivet ikke etablerer nye regler innenfor internasjonal privatrett og heller ikke regulerer spørsmålet om jurisdiksjon. I fortalen punkt 23 utdypes dette til en viss grad ved å fastslå at det ikke er direktivets *mål* å etablere nye regler om lovvalg og jurisdiksjon. Likevel kan en ikke utelukke en analogisk anvendelse av art 3 med interlegal konsekvens. En skal samtidig være forsiktig med å tolke hva som menes med et mål. Artikkel 3 har til hensikt å skape forutberegnelighet for næringsdrivende som ønsker å benytte seg av Internett for å selge innenfor EU/EØS. Denne forutberegneligheten gjelder i forhold til det lands lov en skal forholde seg til ved salg innenfor området. Et annet moment som støtter en innskrenkende tolkning av fortalen punkt 23 er at den selv tilføyer at eksisterende regler i internasjonal privatrett ikke må forhindre fri flyt av varer og tjenester. Dette betyr at hvis eksisterende lovvalgs- eller jurisdiksjonsregler medfører en hindring i forhold til fri flyt av varer og tjenester, vil en se bort i fra disse interlegale reglene i intern rett.

Nå skal det sies at en slik hindring er lite sannsynlig. En av grunnene er at e-handelsdirektivet ikke etablerer nye regler når det gjelder jurisdiksjonsspørsmål, slik at domstolen eller partene må se hen til et lands interne regler utformet i all hovedsak etter Brussel- eller Luganokonvensjonen.[7] Det samme gjelder for lovvalgsspørsmål i kontrakt, som også er unntatt fra art 3. For de fleste EU-land vil slike spørsmål reguleres av reglene i Romakonvensjonen om lovvalg i kontrakt.[8] Derimot kan en stille spørsmålstegn om en potensiell konflikt i forhold til lovvalget utenfor kontrakt hvis domstolens egen rett har lovvalgsregler, f eks for markedsføring, som resulterer i valg av et lands lov som ikke er det samme som i art 3 i e-handelsdirektivet.

Resultatet er at eksisterende lovvalgsregler sjelden vil komme i konflikt med EU/EØS-retten, men der hvor det ikke er lovvalgsregler, slik som lovvalg utenfor kontrakt, vil eksisterende EU/EØS-regler kunne danne grunnlaget for en ny lovvalgsregel. Dette kan sees i lys av art 20 i Romakonvensjonen, som nettopp stipulerer at EU-retten går foran konvensjonens regler.

---

7 Jf 1968 Brussels Convention on Jurisdiction and Enforcement of Judgements in Civil and Commercial Matters (OJ C 189, 1990, 2), og 1988 Lugano Convention on Jurisdiction and Enforcement of Judgements in Civil and Commercial Matters (OJ L 319, 1988, 9).

8 Jf 1980 Rome Convention on the Law Applicable to Contractual Obligations (OJ L 266, 1980, 1). For mer om denne konvensjonen i forhold til lovvalg på Internett, se P Lenda, *Internet and Choice-of-Law*, CompLex 1/2001.

Det er dermed plausibelt å kunne si at e-handelsdirektivet vil kunne påvirke den interlegale retten i Europa i en ny retning. Mens tradisjonell interlegal rett har operert med lovvalgsregler som velger et lands lov etter tilknytningsmomenter som refererer seg til handlinger, f eks hvor en kontrakt er inngått eller hvor en skade er skjedd, tyder det på at den nye retningen bruker tilknytningsmomenter som er mer statiske, dvs at en refererer seg til etableringssteder eller faste tilholdssteder.

4 Etableringsstedet i E-handelsdirektivet

4.1 Problemstilling

I art 3 er etableringsstedet sentralt: En tilbyder av varer eller tjenester on-line må forholde seg til de nasjonale reglene i landet tilbyderen er etablert (jf også art 5 nr 1(b) om informasjon angående tilbyderen).

Hva innebærer et etableringssted på Internett? En som tilbyr tjenester eller varer over Internett trenger ikke nødvendigvis ha et konkret etableringssted, men bare fungere «på nettet». En nettbutikk trenger i prinsippet ikke bestå av annet enn et nettområde som fungerer som et datamaskinprogram med «butikkselgerfunksjoner» gjennom et program (elektronisk agent) som ligger på en server (datamaskin) tilknyttet Internett. Salget av varer eller tjenester skjer gjennom dette nettområdet. Som kjøper vil en da kunne søke etter ønsket vare og få den tilsendt fysisk eller digitalt. Hvis det skjer digitalt trenger ikke initiativtaker foreta seg noen som helst handling, men sitte stille og se at den elektroniske agenten «driver» salget. Hvor den elektroniske agenten er etablert, kan da skape problemer for kjøper hvis denne ønsker å danne seg et bilde av hvor han kjøper tjenesten eller varen fra. Eksempelvis kan det ha seg at serveren hvor den elektroniske agenten ligger, er plassert i land A, mens den som står bak agenten er bosatt i land B, mens nettbutikken har toppdomene fra land C. Hvor tilbyderen da er rettslig sett etablert kan skape problemer.

Hva er så definisjonen av et etableringssted? Den naturlige språklige forståelsen av begrepet tilsier at en som er etablert i et land har en base for sin aktivitet i dette landet. Et eksempel kan her være en som selger varer på postordre. Denne personen vil typisk ha et varelager som varene sendes fra. Selv om personen selger varer over hele Norden, vil denne bli regnet som etablert i det landet hvor varelageret ligger. Enda tydeligere vil dette være ved en som selger på postordre, men også har en faktisk butikk i en by som også fungerer som lager. Mange butikker i Oslo tilbyr varer over hele landet men regnes som etablert i Oslo. Det samme prinsippet må gjelde på Internett.

4.2 Etableringsstedet i EU-retten

Når vi diskuterer hva som menes med etableringssted («establishment») i e-handelsdirektivet, må vi se hen til felleskapsretten der etableringsstedet er et sentralt begrep. Dette gjelder f eks i Romatraktaten tredje del kap 2 om etableringsretten,[9] dog i forhold til e-handel vil ikke Romatraktaten ha den største betydning. Mer relevant er forståelsen av etableringsstedet i fjernsynsdirektivet,[10] personverndirektivet og Brusselkonvensjonen. Disse tre instrumentene har ofte vært nevnt i forhold til e-handel.

Fjernsynsdirektivet

I fjernsynsdirektivet oppstilles det en regel om senderlandets rett. Med dette menes at en tilbyder av tv-sendinger på samme måte som i e-handelsdirektivet må forholde seg til reglene i det landet han sender fra. Det finnes en skranke på dette punktet som gjelder utsendelse som rammer bare et land,[11] men det skal svært lite til for at en tv-kanal ansees for å sende til mer enn et land.[12]

Personverndirektivet

I personverndirektivet oppstilles det også en type regel om senderlandets rett. Mer presist oppstilles det en regel i art 4 om at den som kontrollerer behandlingen av personopplysninger må forholde seg til personvernlovgivningen i det landet han er etablert i. Fortalen punkt 19 fastholder at etablering på en medlemsstats område innebærer faktisk utøvelse av aktiviteter på området gjennom en mer permanent struktur. Når en så vurderer den permanente struktur, vil den rettslige struktur, om det så er en filial eller datterselskap med status som juridisk person, ikke ha avgjørende betydning. For å unngå omgåelse av loven ved etablering i flere medlemsstater skal en sikre at hver enkelt struktur oppfyller kravene i den gjeldende nasjonale lovgivningen. I forhold til e-handelsdirektivet art 3 ser en at etableringsstedet i personverndirektivet setter som vilkår at det foreligger en permanent struktur som tilfredsstiller landets selskapslovgivning. Dette må ventes å gjelde også for e-handelsdirektivet.

---

9 Jf OJ C 340, 10.11.1997, 173.

10 Directive 97/36/EC of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (OJ L 202, 30.7.1997, 60).

11 Jf *TV10 SA v Commissaraat voor de Media*, C-23/93, ECR [1994] 4795.

12 Jf *Konsumentombudsmannen v De Agostini (Svenska) Forlag AB* (C-34/95) og *TV-Shop i Sverige AB* (C-35/95 og C-36/95), ECR [1997] 3843.

Brusselkonvensjonen

I Brusselkonvensjonen er etableringsstedet et særdeles viktig begrep, og det er derfor blitt behandlet flere ganger av EU-domstolen. I Somafer-dommen,[13] som omhandlet fortolkningen av begrepene «branch, agency or other establishment» i konvensjonen art 5(5), ble det opstilt i domsgrunn 12 følgende vilkår for hva som skal regnes som et «place of business»:

> «The concept of branch, agency or other establishment implies a place of business which has the appearance of permanency, such as the extension of a parent body, has a management and is materially equipped to negotiate business with third parties so that the latter, although knowing that there will if necessary be a legal link with the parent body, the head office of which is abroad, do not have to deal directly with such parent body but may transact business at the place of business constituting the extension.»

Mye tyder på at forfatterne av e-handelsdirektivet har hatt denne fortolkning i tankene når de har utferdiget art 3. Det må dog utvises forsiktighet da e-handelsdirektivet spesielt retter seg mot on-line aktivitet og de spesielle forhold som der ligger, mens Brusselkonvensjonen retter seg mot jurisdiksjonsspørsmål, som er unntatt fra direktivet. Likevel er det naturlig å slutte at et etableringssted etter art 3 krever en tilsynelatende grad av fasthet eller stabilitet, har et eget beslutningsorgan og er materielt utrustet til å forhandle med tredjemenn. Et nettområde vil dermed kunne omfavnes dersom det har en avtalemekanisme som skaper en avtale med en potensiell kjøper, dog muligens kun i en interlegal relasjon. Elektroniske agenter vil ofte ha slike mekanismer, spesielt når varen kan lastes ned digitalt etter avtaleslutning og elektronisk betaling.

4.3 Etableringsstedet i e-handelsdirektivet

Hvilke vilkår og definisjoner setter e-handelsdirektivet opp for et etableringssted? I fortalen til direktivet punkt 19 gis det en veiledning. Derav følger det at etableringsstedet må tolkes i overensstemmelse med EU-domstolens rettspraksis.[14] Fortalen oppstiller videre de vilkår som EU-domstolen har gitt i forhold til hva som er et etableringssted. Det sentrale i punkt 19 lyder således:

---

13 *Somafer SA v Saar-Ferngas AG*, C-33/78, ECR [1978] 2183.

14 Fortalen nevner ikke hvor en har hentet rettspraksis fra, men et tidligere forslag til e-handelsdirektivet av 18.11.1998 (COM(1998) 586 final) nevner sak C-221/89 [1991] ECR I-3905.

> «…the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period.»

De sentrale vilkår er dermed at det må foregå (1) faktisk forfølgelse av økonomisk aktivitet gjennom (2) et fast tilholdssted for en (3) ubestemt periode. Hva ligger så i disse vilkårene?

Ad (1): Det må etter min mening foreligge en faktisk aktivitet som har som formål å skape profitt for dem som driver med aktiviteten. En slik tolkning vil for det første skape et skille mot de som etablerer seg på Internett uten faktisk å drive økonomisk aktivitet, men som har et ønske om å gjøre det i fremtiden. For det andre foreligger det en motsetning til de som benytter seg av Internett, men uten noen direkte aktivitet mot en planlagt økonomisk avkastning. Til slutt avgrenser en mot private nettsider, mens ideelle organisasjoner i enkelte tilfeller vil kunne falle innenfor.

Ad (2): Det sentrale ved dette vilkåret angår plasseringen av tilholdsstedet. Her må en se hen til forholdet mellom en økonomisk aktivitet og det stedet hvor denne aktiviteten genereres fra (jf fortalen punkt 19: «…where it pursues its economic activity…»).[15] Spørsmålet er mao hvor kilden til den økonomiske aktiviteten ligger. Hovedregelen må være at et selskap skal forholde seg til reglene i det land hvor selskapet er registrert. I tilfeller hvor det ikke foreligger et registrert selskap bak den økonomiske aktiviteten, f eks en person som på privat basis driver en betalingstjeneste over Internett, vil en her ta denne personens bosted som det land hvor den økonomiske aktiviteten originerer fra. Dette er også i overensstemmelse med allerede eksisterende regler i Brussel/Lugano konvensjonen(e) og Romakonvensjonen. At en her ser etter stedet hvor aktiviteten kommer fra, kan også leses fra fortalen til e-handelsdirektiv punkt 22, som henviser til «the source of the activity» og «where the services originate».

En kan spørre seg om en elektronisk agent – noe forenklet et datamaskinprogram som utfører automatiserte handlinger med en viss grad av autonomi – kan representere et fast tilholdssted, dvs et etableringssted. Forholdet til elektroniske agenter er ikke direkte berørt i direktivet. Likevel berører direktivet forholdet til IKT. Artikkel 2c annet punktum slår fast at en tjenestetilbyders etableringssted ikke vil være bestemt av tilstedeværelse og bruk av teknologier som muliggjør tjenesten. Disse kan mao ikke i seg selv utgjøre et etableringssted. Fortalen punkt 19 gjør det klart at en som tilbyr tjenester via

15 Fortalen sier at en må forholde seg til stedet der tilbyderen "pursues its economic activity". Isolert sett kunne en her si at en dermed legger vekt på det stedet hvor tilbyderen forfølger sin økonomiske aktivitet, altså det stedet en tilbyr tjenester over Internett. Dette ville imidlertid ikke være i overenstemmelse med art 3 eller fortalen punkt 22 (se nedenfor), og dermed mener jeg at en må se hen til stedet hvor den økonomiske aktiviteten originerer fra.

et nettområde ikke er etablert på det stedet hvor nettområdet er teknisk plassert eller hvor nettsiden er tilgjengelig, men snarere hvor tjenesten originerer fra. Selv om en plasserer et nettområde på en server i et annet land enn det landet hvor bedriften er etablert, vil plasseringen ikke ha betydning i denne sammenhengen. En elektronisk agent vil falle inn under denne type teknologier, siden den vil oftest være integrert med nettområdet og samtidig være et sentralt element i den teknologiske gjennomføringen av tilbydelsen. I tillegg er det klart at et nettsted alltid vil være programmert av noen som har kontroll med hvordan det fungerer. Stedet hvor denne personen eller organisasjonen er etablert, kan sies å være stedet hvor nettstedet eller den elektroniske agenten originerer fra. Konsekvensen er at bruken og plasseringen av teknologiske hjelpeelementer, servere eller elektroniske agenter, ikke har betydning i forhold til hvor en tilbyder av Internettjenester er etablert. Det sentrale er hvor bedriften er etablert eller i mangel av et etablert selskap, bostedet til personen bak nettområdet. Det må dog utvises en viss ydmykhet overfor fremtidens teknologier, slik som intelligente agenter; disse agentene kan komme til å ha en tilstrekkelig grad av autonomi til at de forholdsvis lett kan utgjøre et etableringssted.

Skulle det være flere etableringssteder – noe som fortalen punkt 19 forutsetter – skal en legge til grunn etableringsstedet til den som har ytt tjenesten. Hvis det ikke kan bestemmes hvilke som har ytt tjenesten så skal en legge til grunn det stedet som regnes for å være sentrum for aktiviteten. På mange måter ligner dette på den «nærmeste tilknytning»-metode som brukes i internasjonal privatrett.[16] Fremgangsmåten kan være aktuell i forhold til virtuelle selskaper – dvs selskaper hvor deltagerne slutter seg sammen gjennom Internett for en bestemt periode og leverer et digitalt produkt. Slike konstellasjoner gjør det vanskelig å bestemme hvor sentrum for en bestemt aktivitet foreligger.

Ad (3): Fortalen punkt 19 presiserer at vilkåret om at etableringsstedet må foreligge for en ubestemt periode også vil være oppfylt når etableringsstedet foreligger for en bestemt periode. Et typisk eksempel på en bedrift som er etablert for en bestemt periode kan finnes i den digitale verden hvor virtuelle selskaper dannes i prosjektformål over landegrensene.

For å konkludere om hva som menes med et etableringssted for en «informasjonssamfunnstjeneste-tilbyder» må en skille mellom det tilsynelatende og det faktiske. Det må ikke søkes etter de tekniske disposisjoner som foreligger, men snarere den statiske tilstedeværelsen av et fysisk sted. Dette stedet vil enten være det hvor et selskap er etablert og driver sin økonomiske aktivitet

16 Jf bl a Irma-Mignon dommen, Rt 1923 II 59.

fra, eller bostedet til den personen som driver samme type aktivitet. Plassering på servere eller tekniske forsøk på å fjerne seg fra et slik sted, vil ikke ha noen betydning.

5 Det koordinerte området

5.1 Innledning og definisjon av det koordinerte området

Regelen i art 3 kommer til anvendelse kun innenfor «the coordinated field» eller som det betegnes i den danske versjonen «det området, der er koordinert ved dette direktiv». Når en allerede vet at direktivet bare får anvendelse som et supplement til allerede eksisterende regler, samtidig som regelen begrenses av regler om personvern, offentlig helsevern mv, kan det reises spørsmål om regelen i det hele tatt får noen stor praktisk betydning.

Hva er så det koordinerte området? Direktivet art 2h definerer det koordinerte området som:

> «requirements laid down in Member States' legal systems applicable to Information Society service providers or Information Society services, regardless of whether they are of a general nature or specifically designed for them».

Fortalen punkt 21 tilføyer at det koordinerte området bare dekker «requirements relating to on-line activities». Som eksempel nevnes «…on-line advertising, on-line shopping, on-line contracting…», mens krav til varene, deres sikkerhetsstandarder og lignende ikke dekkes. En midlertidig konklusjon må således være at det koordinerte området dekker alle krav som relaterer seg til on-line aktiviteter. En naturlig forståelse av ordlyden vil her kunne være at det henvises til alle rettsregler i et land som setter skranker for tilbydere av informasjonssamfunnstjenester.

Hva menes så med *krav* («requirements»)? Utgangspunktet må være at det henvises til rettsregler, slik som formell lov, forskrifter eller annen etablert praksis som har relevans på informasjonssamfunnstjenester. Her må det spørres om hvorvidt krav bare omfavner krav i forhold til etableringen og dermed oppstarten av en informasjonssamfunnstjeneste og ikke krav i forhold til tjenestens videre drift. Det er klart at siktemålet med direktivet er å fjerne hindringer for utviklingen av e-handel og at etablering er ofte det viktigste momentet i den forbindelse. Likevel vil jeg her helle mot å tolke rettskrav som alle rettsregler som berører informasjonssamfunnstjenester. Hvis en tillater etablering av en slik tjeneste, men samtidig har hindringer i den daglige driften, vil oppstarten være til liten nytte.

Det neste spørsmålet er hvilke rettsfelt som inkluderes i disse krav, annet enn at det retter seg mot informasjonssamfunnstjenester. Ifølge art 2h(i) gjelder «requirements» de regler en tilbyder må overholde for å kunne bedrive sin aktivitet. Dette gjelder for det første regler som tillater tilbyderen å bedrive sin aktivitet, slik som regler om kvalifikasjoner, autorisasjoner eller notifikasjoner. For det andre, og kanskje viktigere, presiseres det at «requirements» også henviser til de regler som gjør seg gjeldende i forfølgelsen av aktiviteten, dvs tilbydelsen. Dette eksemplifiseres gjennom regler som omhandler kvaliteten eller innholdet av tjenesten og som inkluderer de regler anvendelig på reklame og kontrakter, eller de regler som relaterer seg til tjenestetilbyderens ansvar. Dette medfører at art 3 i utgangspunktet gjelder for de fleste sider av e-handelen. En tjenestetilbyder kan reklamere på Internett, utferdige kontrakten, og være ansvarlig for feil ved disse sider etter reglene i landet han er etablert.

Artikkel 2h(ii) setter dog visse skranker til art 2h(i). Her gjøres det klart at det koordinerte området ikke dekker kravene til varene i seg selv. Den fastslår videre at art 3 ikke gjelder for reglene om levering av varene. Til slutt avgrenses det mot regler som gjelder for tjenester som ikke leveres elektronisk. Det koordinerte området begrenses mao til de sider som gjelder den elektronisk delen av enhver handel. Disse begrensningene kommer på toppen av flere andre begrensninger til direktivets anvendelsesområdet generelt (jf avsnitt 2 ovenfor og avsnitt 5.2 nedenfor). Likevel kan en si at direktivet i utgangspunkt skaper en stor grad av forutberegnelighet for en tilbyder av tjenester over Internett. Tilbyderen kan i sin «digitale form» i stor grad forholde seg etter reglene i det landet han er etablert eller bosatt.

5.2 De relative unntakene til det koordinerte området

Viktige begrensninger på hva som omfattes av det koordinerte området finner vi i Art 3 nr 3 og nr 4. Sistnevnte stipulerer at en medlemsstat kan derogere fra bestemmelsen i art 3 nr 2 under visse vilkår. Derogasjonen kan imidlertid skje bare på individuell basis, dvs i forhold til en bestemt informasjonssamfunnstjeneste. Det kan mao ikke foreligge en generell regel som forbyr en gruppe eller en type tjenester. Dette kan nok i praksis vise seg å være et viktig vilkår.

Andre vilkår for at derogasjon kan oppstilles etter art 3 nr 4 er at tiltaket er (i) nødvendig av offentlig hensyn slik som f eks å forhindre rasisme, eller beskytte offentlig helse, offentlige og nasjonale sikkerheten eller forbrukerhensyn inkludert investorer. Samtidig skal derogasjon bare skje (ii) mot en bestemt informasjonssamfunnstjeneste som avviser forhold nevnt under (i) eller som står i alvorlig og seriøs fare for å gjøre det. Til slutt (iii) må tiltak som skal beskytte interessene nevnt i (i) være proporsjonale i forhold til for-

målet og ikke gå lenger enn hva som er nødvendig for å oppfylle vernet (jf fortalen punkt 10). Disse vilkår følger også av Romatraktaten.

Det oppstilles også visse prosessuelle regler for hvordan derogasjon kan skje (jf art 3 nr 4(b) og nr 5). Disse behandles ikke her.

Kanskje det mest sentrale i forhold til art 3 er likevel at på de områder som formelt sett er harmonisert av felleskapsretten, nemlig de områder som dekkes av de direktiv som er nevnt i fortalen punkt 11, vil det kreves mye for at tiltak etter art 3 nr 4 kommer til anvendelse. Reglene som er nevnt i fortalen punkt 11 er nokså omfattende. De dekker mange viktige sider ved forbrukervern. Rettspraksis fra EU-domstolen viser at det ikke er lett for en medlemsstat å innføre lovlig derogasjon fra harmoniserte minimumsstandarder.[17]

5.3 De absolutte unntakene til det koordinerte området

Andre unntak fra art 3 nr 1 og 2 er statuert i nr 3, som slår fast at art 3 nr 1 og 2 ikke kommer til anvendelse på de felter som nevnes i anneksen til direktivet. Anneksen oppstiller åtte slike felter. Disse dekker bl a visse opphavsrettslige regler, visse regler om tilbydelse av finansielle tjenester og forsikring, forbrukerkontrakter, og regler om lovvalget i kontrakten. Anneksen nevner også regler om lovligheten ved uoppfordret tilsendelse av e-mail. Slik tilsendelse skal reguleres gjennom personverndirektivet. Derimot vil art 3 kunne komme til anvendelse når det gjelder reklamen i utsendelsen, hvis utsendelsen er lovlig eller oppfordret.

6 Konklusjon

Isolert sett fremstår hovedregelen i art 3 som en «country of origin»-regel som er ment å skape forutberegnelighet for den som er tilbyder over elektroniske nettverk. Dette bildet er imidlertid nokså unyansert av flere grunner.

For det første gir et slikt bilde ikke nok plass til det faktum at regelen følger hovedprinsippet i Romatraktaten om fri flyt av varer og tjenester med det mål å etablere et indre marked. Som sådan representerer art 3 ikke en ren interlegal regel.

For det andre er regelen bare ment å fungere innenfor det koordinerte området. I dette området finnes det felleskapslovgivning som ikke kan begrenses av e-handelsdirektivet.

For det tredje kommer ikke e-handelsdirektivet til anvendelse på enkelte områder, slik som opphavsrett, visse forsikringsavtaler og det materielle innholdet i forbrukerkontrakter.

---

17 Jf De Agostini-sakene, referert i fotnote 12.

For det fjerde kan medlemsstatene komme med tiltak mot regelen i art 3 nr 1 og 2 for å verne om visse interesser, slik som offentlig helse og forbrukervern. Derogasjonen må likevel være proporsjonalt i forhold til dens formål, og muligheten for slik derogasjon vil være begrenset på områder der EU har utstedt harmoniserte minimumsstandarder.

Utgitt i CompLex-serien

CompLex er Institutt for rettsinformatikks skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra GnistAkademika (se bestillingsskjema bak i boken), eller lånes på biblioteket. CompLex-serien ligger i BIBSYS.

2001

1/01 **Internet and Choice-of-Law - The International Sale of Digitised Products through the Internet in a European Context**
Peter Lenda.....*NOK 275.-*

2/01 **Internet Domain Names and Trademarks**
Tonje Røste Gulliksen.....*NOK 227.-*

3/01 **Internasjonal jurisdiksjon ved elektronisk handel - med Lugano-konvensjonen art 5 (5) og elektroniske agenter som eksempel**
Joakim S. T. Øren.....*NOK 204.-*

4/01 **Legal issues regarding virtual organisations**
Emily M. Weitzenböck..... *NOK 164.-*

5/01 **Cyberspace jurisdiction in the U.S. - The International Dimension of Due Process**
Henrik Spang-Hanssen.....*NOK 685.-*

6/01 **Norwegian Border Control In A Europe Without Internal Frontiers. -Implications for data protection and civil liberties**
Stephen Kabera Karanja.....*NOK 252.-*

2000

1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange ..... *NOK 268.-*

2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth ..... *NOK 248.-*

3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll ..... *NOK 148.-*

1999

1/99 **International regulation and protection of Internet domain names and trademarks**
Tonje Røste Gulliksen ..... *NOK 248.-*

2/99 **Betaling via Internett**
Camilla Julie Wollan ..... *NOK 268.-*

3/99 **Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog ..... *NOK 198.-*

1998

1/98 **Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen ..... *NOK 198.-*

2/98 **Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik ..... *NOK 238.-*

3/98 **Interconnection - the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu ..... *NOK 198.-*

1997

1/97 **Eksemplarfremstilling av litterære verk til privat bruk**
Therese Steen .....*NOK 158.-*

2/97 **Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam .....*NOK 175.-*

3/97 **Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen .....*NOK 170.-*

4/97 **Private pengespill på Internett**
Halvor Manshaus.....*NOK 160.-*

5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh.....*NOK 255.-*

6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing.....*NOK 178.-*

7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad *NOK148.-*

8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen.....*NOK 120.-*

9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen .....*NOK 168.-*

10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida.....*NOK 140.-*

11/97 **Rettslig vern av databaser**
Harald Chr Bjelke.....*NOK 358.-*

1996

1/96: Innsynsrett i elektronisk post i offentlig forvaltning
Knut Magnar Aanestad og Tormod S. Johansen.....*NOK 218.-*

2/96 Public Policy and Legal Regulation of the Information Market in the Digital Network Enviroment
Stephen John Saxby .....*NOK 238.-*

3/96 Opplysning på spill
Ellen Lange.....*NOK 218.-*

4/96 Personvern og overføring av personopplysninger til utlandet
Eva I. E. Jarbekk .....*NOK 198.-*

5/96 Fjernarbeid
Henning Jakhelln .....*NOK 235.-*

6/96 A Legal Advisory System Concerning Electronic Data Interchange within the European Community
Andreas Mitrakas.....*NOK 128.-*

7/96 Elektronisk publisering: Utvalgte rettslige aspekter
Jon Bing og Ole E. Tokvam .....*NOK 186.-*

8/96 Fjernsynsovervåking og personvern
Finn-Øyvind H. Langfjell.....*NOK 138.-*

1995

1/95 Rettslige konsekvenser av digitalisering: Rettighetsadministrasjon og redaktøransvar i digitale nett
Jon Bing.....*NOK 368.-*

2/95 Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon
Sverre Sandvik .....*NOK 178.-*

3/95 **Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith.....*NOK 278.-*

4/95 **Personvern og straffeansvar - straffelovens § 390**
Ole Tokvam.....*NOK 198.-*

5/95 **Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs.....*NOK 138.-*

6/95 **Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum.....*NOK 348.-*

7/95 **Law and Liberty in the Computer Age**
Vittorio Frosini.....*NOK 158.-*

1994

1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed).....*NOK 358.-*

2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen.....*NOK 318.-*

3/94 **Elektronisk datutveksling i tollforvaltingen - Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs.....*NOK 225.-*

4/94 **Sykepenger og personvern - Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad.....*NOK 148.-*

5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand.....*NOK 148.-*

6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing.....*NOK148.-*

7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand ..... *NOK 138.-*

8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red) ..... *NOK 158.-*

9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke ..... *NOK 198.-*

10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)**
Gjert Melsom ..... *NOK 198.-*

1993

1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor ..... *NOK 148.-*

2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt ..... *NOK 138.-*

3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer ..... *NOK 178.-*

4/93 **Consumers Purchases through Telecommunications in Europe. - Application of private international law to cross-border contractual disputes**
Joachim Benno ..... *NOK 198.-*

5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal ..... *NOK 218.-*

6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen ..... *NOK 148.-*

7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind ..... *NOK 158.-*

1992

1/92 **Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesseltvedt .....*NOK 138.-*

2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland .....*NOK 208.-*

3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm.....*NOK 228.-*

4/92 **Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret**
Ditlev Schwanenfügel.....*NOK 158.-*

5/92 **Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal .....*NOK 248.-*

6/92 **Implementing EDI - a proposal for regulatory form**
Rolf Riisnæs.....*NOK 118.-*

7/92 **Deponering av kildekode«escrow»-klausuler TERESA (79)**
Morten S. Hagedal .....*NOK 128.-*

8/92 **EDB i juridisk undervisning – med en reiserapport fra England og USA**
Ola-Kristian Hoff.....*NOK 228.-*

9/92 **Universiteters ansvar for bruk av datanett TERESA (94)**
Jon Bing & Dag Elgesem .....*NOK 198.-*

10/92 **Rettslige sider ved teletorg**
Andreas Galtung.....*NOK 148.-*

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Navn: _____
Adresse: _____
Postadresse: _____
Telefon: _____

Bestillingsskjemaet sendes pr.post eller telefaks til:

gnist akademika
Fagbokhandelen i Oslo

Avd. juridisk litteratur Aulabygningen
Karl Johansgt. 47, 0162 Oslo
Telefon: 22 42 54 50
Telefaks: 22 41 17 08

CompLex kan også bestilles via nettbokhandelen www.gnist.no