Georg Philip Krog og Anne Gunn B. Bekken (red.)

YULEX 2005

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 82-7226-094-8
ISSN 0806-1912

unipubskriftserier

Utgitt i samarbeid med Unipub AS
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: e-dit AiT AS
Omslagsdesign Kitty Ensby

Institutt for rettsinformatikks utgivelser i skriftserien Complex er støttet av:
Advokatfirmaet Selmer DA
Wikborg Rein & Co
Lovdata

CONTENTS

Forord 5

Preface 5

Jon Bing
1 Kunnskap 7

Dag Wiese Schartum
2 Notater om å ivareta informasjonssikkerhet ved hjelp av regelverk 13

Arild Jansen
3 Assessing E-government progress – why and what 37

Thomas Olsen, Tobias Mahler (m.fl.)
4 Privacy in Relation to Networked Organisations and Identity Management 57

Tobias Mahler (medforfatter: Fredrik Vraalsen, SINTEF)
5 Legal Risk Analysis with Respect to IPR in a Collaborative Engineering Virtual Organization 69

Stephen K. Karanja
6 SIS II Legislative Proposals 2005: Gains and Losses! 81

Dejan Jovanovic
7 Public Administration in the Republic of Serbia: Competence, Organization and Reform 105

Yue Liu
8 Electronic Discovery: The Management and its Application 143

Emily M. Weitzenböck
9 Good Faith and Fair Dealing in Contracts Formed And Performed by Electronic Agents 181

Maryke Silalahi Nuth
10 Article 11 of the Electronic Commerce Directive: A failed attempt to harmonise electronic contract formation? 213

Inger Marie Sunde
11 Politi, pirateri og kodeknekking 227

Georg Philip Krog
12 Jurisdiksjon og avgrensning av Internett`s kolliderende handlingsuniverser 249

FORORD

Denne boken er den femte i Yulex-serien. Siktemålet med serien er å tilby venner av Institutt for rettsinformatikk smakebiter fra ulike temaer som har opptatt instituttets medarbeidere i løpet av dette året.

De fleste av årets artikler har enten vært publisert eller fremført som foredrag i internasjonale fora.

Opplysninger om forfatterne er tilgjengelig på
http://www.jus.uio.no/iri/om_iri/folk/index.html

God jul og fornøyelig lesning!

Georg Philip Krog og Anne Gunn B. Bekken

PREFACE

This book is the fifth in the Yulex series. The aim with the series is to offer friends of the Norwegian Research Center for Computers and Law a "Christmas smorgasbord" of the various themes upon which Centre staff have been working over the past year.

Most of this years articles have either been published or presented in international fora.

Information about the authors is available at
http://www.jus.uio.no/iri/english/nrccl/people/index.html

Merry Christmas and happy reading!

Georg Philip Krog and Anne Gunn B. Bekken

1 KUNNSKAP

Jon Bing

"Kunnskap" er et ord fra dagligspråket som også kan brukes i en teknisk betydning. Dette notatet har ingen pretensjoner om å være fagfilosofisk eller på annen måte en betraktning utover en refleksjon bygget på lang omgang med begrepet 'kunnskap'[1] Fordi ordet er så mye brukt i både dagligdags språk og i tekniske sammenhenger, har det tilsvarende mange betydninger. I daglig språk vil ordets betydning i stor grad bestemmes av sammenhengen, og derfor skifte – ofte innen det samme dokument eller den samme samtalen.[2] I teknisk forstand gjøres det definisjoner som til dels er svært forskjellige mellom ulike disipliner.

I dette notatet er pretensjonen ikke å diskutere "kunnskap" rent generelt. Men "kunnskap" er et så generelt ord at man ofte har hatt behov for å presisere det, å snakke om ulike former for kunnskap.

I utgangspunktet er "kunnskap" et ord som er beslektete med ord som "tanke" eller "følelse". Det betegner derfor noe som vi alle sammen "vet hva er" fordi vi selv opplever det og mer enn det – det er på en måte en del av oss, nærmest det som definerer vår egen identitet. Samtidig er dette betegnelser på noe som er "inne" i oss, og som derfor ikke originært kan oppfattes av andre mennesker. Vi kan rapportere om vår kunnskap, men vi

1 Når et ord brukes mellom enkle hermetegn (') siktes det til ordets semantiske betydning, når det brukes med vanlige hermetegn (") siktes det til ordets syntaktiske betydning eller rolle. I dette notatet spiller knapt denne formalismen noen rolle, og er sikkert unødvendig presiøst.

2 Jurister omtaler av og til ordets "naturlige betydning" eller forsøker på andre måter å angi at et ord har en betydning uten sammenheng, nærmest som om betydningen ligger i en skuff merket med ordet selv, og som man så kan trekke ut for å titte på hvilken betydning dette uttrykket har. Det er uriktig. Ord forekommer alltid i en sammenheng, selv når de står som oppslagsord i en ordbok ("norsk-italiensk") forutsettes det en sammenheng. Og skulle man ønske å bruke utenfor en slik sammenheng, kan man få interessante overraskelse, selv om man ikke griper til bruk av homonymer eller –grafer.

kan ikke vise den frem på annen måte enn nettopp rapporten.[3] Vi kan snakke om "ny kunnskap" i den betydningen at dette var noe vi ikke "visste" fra før, men hvem vet egenlig det? Utsagnet er en rapport fra vårt indre liv som andre må tro på eller mistro. Wittgenstein har formulert det i en slags aforisme:[4] "Hva er forskjellen mellom en mann som *sier* han har vondt i armen, men som ikke har det, og en mann som *sier* han har vondt i armen, og virkelig har det?"

Hvis man på denne måten begynner å reflektere over begrepet kunnskap, kan man lett oppleve det som komplisert og merkverdig. I og for seg er vel det riktig, for man får fatt i en snipp av den duken som gjør mennesket til et merkverdig og sammensatt vesen, som vi gjennom vitenskap og kunst aldri blir ferdig med å reflektere over. Det gjør det også på en måte litt nytteløst å fatt på oppgaven som så mange innsiktsfulle filosofer og kunstnere ikke er blitt ferdig med.

Derfor får man i praksis nøye seg med å konstatere at man har behov for å snakke om ulike aspekter av kunnskap, og at man kan gjøre det uten å skritte ut i de store avgrunnene av filosofisk karakter.

Man kan hevde at kunnskap har tre kilder. Det er for det første (primært) de erfaringer man selv gjør gjennom arbeid, lek og samvær med andre. Det er for det andre (sekundært) det man blir fortalt av en annen person som er til stede, og som forteller om reiser, barndom eller egne erfaringer, og som man kan spørre om nærmere forklaringer fra. Det er for det tredje (tertiært) kunnskap man får ved å lese bøker, høre på radio eller foredrag, se på fjernsyn osv – dvs fra media hvor "avsender" ikke er til stede i situasjonen. Alt dette avleirer seg som "kunnskap" hos den som mottar inntrykkene.

Det er da lett å se at disse kildene til kunnskap kan være kvalifisert på ulik måte, dramatisert ved at man leser søsterens dagbok, at man dirket opp et arkivskap om leser hemmelige dokumenter osv.

Det er nettopp ved å rette oppmerksomheten mot *hvordan* man har fått kunnskapen, at man kan nærme seg en karakteristikk, om ikke en definisjon, av know-how.

Know-how er først og fremst et eksempel på "primær kunnskap", altså slik kunnskap man har vunnet ved egne erfaringer. Men disse erfaringene er vunnet fordi andre enn en selv har iscenesatt situasjoner hvor erfaringene kan høstes.

Et mye brukt eksempel er fra helsevesenet, hvor en yngre helsearbeider følger en eldre på rundende blant pasienter. Det er dokumentert at erfarne helsearbeidere kan oppdage tegn til problemer – og dermed treffe tiltak for

3 Rapporten betegnes som "data", altså tegn eller signaler som ved hjelp av en formalisme (som et språk) er egnet til å bære kunnskap fra ett menneske til et annet. I forhold til dette notatet synes det unødvendig å gå nærmere inn på dette forholdet, som i seg selv bygger på en egen teori om "kunnskap".

4 Som feilsiteres etter hukommelsen.

å hindre at problemene forverrer seg – uten at verken vedkommende helsearbeider eller den yngre kollegaen kan forklare hvilke ytre tegn som røpet den kritiske tilstanden. I dagligtale dekkes dette ofte over med å si at man er "erfaren" eller har "intuisjon".

Faglig er det en diskusjon om hva slags kunnskap dette representerer. Enkelte hevder at det er kunnskap som prinsipielt ikke kan forklares i ord eller på andre måter formidles til andre fordi språket (eller hva man ellers har til rådighet for å formidle kunnskap) rett og slett mangler ord (eller andre former for tegn eller signaler). Likevel vil den yngre kollegaen lære fra den eldre hva som var det relevante etter mange netters samvær, selv om den yngre heller ikke da vil være i stand til å fortelle hva han eller hun har lært.

Dette kalles gjerne spørsmålet om "tacit knowledge" eller "tyst kunnskap". Som nevnt er det en skole som mener dette representerer kunnskap som prinsipielt ikke lar seg formidle med ord (eller andre tegn eller signaler). En annen skole[5] mener at det bare er "vanskelig" å formidle kunnskapen, men ikke "umulig".

Relasjonen mellom den eldre og den yngre helsearbeideren blir ofte uttrykt som relasjonen mellom en mester og en svenn, og det er nok fra disse relasjonene man har de fleste studiene.

Men hvis man ser på situasjonen prinsipielt, så har man altså det forholdet at en "mester" har en viss kunnskap som vedkommende ønsker å formidle til en "svenn". Mesteren mangler ord for å fullføre denne formidlingen, så han sier rett og slett: "Følg meg." Slik overføres kunnskapen, som vil være et typisk eksempel på know-how.

Men åpenbart kan vi forandre eksempelet. Mange av oss vil ha erfaringer fra situasjoner hvor vi første gang vi forsøkte å gjøre det, fant det vanskelig – til en situasjon etter langvarig frustrasjon ikke lenger opplever det som vanskelig. Et typisk eksempel vil være en nøkkel i en lås, nøkkelen må inn akkurat langt nok for å gå rundt, men ikke for langt. Antakelig vil erfaringer fra hotellbesøk med gammeldagse nøkler være tilstrekkelig til å vekke minner som kan illustrere akkurat dette poenget.

Og slik vil det også være med oppgaver hvor det er *arbeidsgiver* som gir en arbeidstaker nøkkelen og ber vedkommende åpne låsen. Første gang går det ikke og arbeidstakeren sliter og strever og lærer (uten riktig å vite hva han eller hun lærer) inntil vedkommende en dag kan si: "Åpne låsen? Naturligvis."

Tacit knowledge. Erfaring. Knowhow.

Naturligvis får man ikke forenkle denne situasjonen og hevde at vedkommende har "kunnskap". Det er helt korrekt – naturligvis – at vedkommende har kunnskap, men det er ikke irrelevant *hvordan* vedkommende har fått denne kunn-

5 Og det spiller selvsagt i sammenhengen ingen rolle at jeg bekjenner meg til denne.

skapen. Hadde vedkommende dirket opp en arkivskuff og lest hemmelige dokumenter, ville de fleste innsett at gjenbruk av kunnskap ervervet på denne måten ikke ville vært akseptabelt. Det kommer bl a av at dette er et eksempel på *tærtiær* kunnskap, som lettere lar seg identifisere på grunn av måten den erverves.

Men det blir vanskeligere når kunnskapen er ervervet ved hjelp av egne erfaringer, når det er *kombinasjonen* av oppdrag og egen gjennomføring av oppdrag, en gjennomføring som typisk skjer i samarbeid med andre, som alle arbeider for å fullføre et oppdrag gitt av arbeidsgiver.

I dette siste ligger det også et poeng. For 'kunnskap' forestilles gjerne som noe "inne i hodet" på et enkelt menneske. Det er utilstrekkelig for å forklare hvordan flere, av og til mange, klarer å samarbeide slik at en oppgave løses. Det er nettopp gjennom samarbeidet at den enkelte har ervervet innsikt og kunnskap. Og uten dette samarbeidet, ville vedkommende aldri "lært" det som samarbeidet har gitt vedkommende av individuell kunnskap.

Derfor kan vedkommende gå ut av samarbeidet, ta med seg sin skjerv av 'kunnskap' og omsette den i verdi hos en ny arbeidstaker eller oppdragsgiver. Dette er det gledelige og byggende i ervervelse av kunnskap.

Den negative siden av dette er selvsagt at den knowhow som erverves gjennom møysommelig og tidkrevende samarbeid på en arbeidsplass blir forsøkt utnyttet ved en annen, hvor snarveien gjennom usynlige, men ervervede erfaringer forbikjører nødvendige investeringer.

Det problematiske med "knowhow" er at det er en form for primær kunnskap. Den er ervervet på samme måte som den enkelte har vunnet sin faglige innsikt, den kunnskap som nettopp er den vedkommende tilbyr en arbeids- eller oppdragsgiver. Forskjellen er likevel i to forhold:

- Kunnskapen er vunnet gjennom arbeidsgiverens oppdrag og plan. Uten at arbeidsgiver hadde hatt et slikt oppdrag – kall det gjerne en visjon – ville ikke den ansatte (oppdragstakeren) plassert seg i en situasjon om gjorde det mulig å høste denne erfaringen (kunnskapen).
- Kunnskapen er typisk vunnet i samarbeid med andre i samme organisasjon eller oppdrag. Den er derfor ikke et resultat av "selvstudier", men et resultat av organisert samarbeid – en organisering som arbeidstakeren selv typisk ikke har tatt initiativ til, men som er satt i scene av arbeidsgiver.

Samtidig må det være klart at det nettopp er gjennom arbeid med oppgaver stilt av arbeidsgiver at en arbeidstaker vinner erfaring, vedlikeholder og legger til sin kunnskap. Det er selvsagt denne kunnskapen (i sin generelle og svært diffuse mening) som arbeidstakeren skal kunne bruke for å promotere seg selv, eller bruke som argument for at en annen arbeidsgiver bør ansette nettopp

ham eller henne. De fleste av oss er nok ansatt i tiltro at våre kunnskaper kan være av verdi for arbeidsgiver, ikke fordi vårt vakre ansikt eller sterke armer vil ha betydning for arbeidsgivers virksomhet.

2 NOTATER OM Å IVARETA INFORMASJONSSIKKERHET VED HJELP AV REGELVERK[1]

Dag Wiese Schartum, Avdeling for forvaltningsinformatikk (AFIN), UiO

1 Introduksjon

I dette notatet vil jeg presentere synspunkter på informasjonssikkerhet og regelverk som regulerer slik sikkerhet. Jeg vil dessuten skissere enkelte mulige arbeidsmåter som kan antas å være til nytte i det videre arbeidet med å forbedre informasjonssikkerhetsregelverket i Norge. Notatet referer ikke til andres arbeider, men prøver å se på spørsmål vedrørende regelverk for sikring av informasjon med "friske øyne". Samtidig er det imidlertid klart at deler av notatet er inspirert av resultater fra andres arbeid. Særlig gjelder dette arbeidet som forsker Are Vegard Haug ved Avdeling for forvaltningsinformatikk har utført vedrørende kartlegging og diskusjon av sikkerhetsregelverk.[2]

I første avsnitt av notatet diskuterer jeg hva informasjonssikkerhet og informasjonssikkerhetsregelverk er. Dette er et spørsmål som mange muligens vil mene har opplagte svar, men som jeg antar bør drøftes for lettere å kunne identifisere de deler av informasjonssikkerhetsarbeidet som bør prioriteres. I avsnitt 3 skisserer jeg en modell for regelverksarbeid som etter min mening er anvendelig for arbeidet med sikkerhetsregelverk. Denne modellen forutsetter bruk av teknikker, verktøy og organisering som virkemidler i de ulike trinnene i arbeidet med regelverk. Regelverk som pålegger plikter eller innskrenker rettigheter og som dessuten er ressurskrevende å etterleve for "pliktsubjektene" vil lett skape motsetningsforhold. I avsnitt 4 gjør jeg en enkel beskrivelse av mulige hovedmotsetningsforhold i sikkerhetsarbeidet, og antyder noe om mulige implikasjoner for valg av reguleringsstrategi. I avsnitt 5 drøfter jeg med bakgrunn i slike eventuelle motsetninger, og mulige implikasjoner for utforming av regelverk som kan sikre mest mulig effektiv styring (avsnitt 5). Resten av notatet (avsnittene 6 – 8) inneholder skisser av slik virkemiddelbruk som jeg forutsetter i

1 Notatet er utarbeidet som ledd i arbeid i arbeidsgruppen Regelverk og informasjonssikkerhet, nedsatt av Koordineringsutvalget for informasjonssikkerhet (KIS). Notatet er også publisert som kapittel 5 i arbeidsgruppens rapport av 7. juni 2005.

2 Haugs arbeid var ultimo mai 2005 under ferdigstilling for publisering.

modellen for regelarbeidet i avsnitt 4. Stikkord her er teknikker for samordning av regelverk (avsnitt 6), verktøy for forarbeider, regelanvendelse og evaluering (avsnitt 7), og organisering av rettsanvendelsen (avsnitt 8). Avslutningsvis gir jeg noen råd om det videre arbeidet med informasjonssikkerhetsregelverk.

Det er grunn til å minne om at fremstillingen langt fra representerer noen uttømmende analyse. Hensikten er å gi innspill som kan gi idéer til utvikling av og forskning på informasjonssikkerhetsregelverk. Notatet er diskutert i et møte i arbeidsgruppen for regelverk og informasjonssikkerhet, men innholdet står helt og fullt for forfatterens regning.

2 Allment om regelverk vedrørende informasjonssikkerhet

Informasjonssikkerhetsregelverk betegner – naturlig nok – regelverk som skal sikre informasjon. Noen ganger brukes også betegnelsene "datasikkerhet" og "datasikkerhetsregler". Ut i fra et vanlig skille mellom informasjon og data, kan det være naturlig å legge noe forskjellig mening i de to begrepene.[3] Til tross for en mulig meningsforskjell, velger jeg her å oppfatte datasikkerhet og informasjonssikkerhet som – i utgangspunktet – synonyme begreper. Imidlertid ser det ut til å være "informasjonssikkerhet" som er den dominerende betegnelsen for de relevante regelverkene som er vedtatt de siste 10 årene. "Informasjonssikkerhet" ser samtidig ut til å betegne regelverk som representerer helhetlige tilnærminger til informasjonssikkerhet. Med det mener jeg at ambisjonen er å ivareta de tre tradisjonelt viktigste sikkerhetsaspektene (konfidensialitet, integritet og tilgjengelighet), og at det anvendes mange tiltakstyper for å sikre informasjonen (organisatoriske, tekniske, fysiske osv). I de siste årene er "datasikkerhet" lite anvendt i regelverk, og har tidligere mest blitt brukt om enkeltstående bestemmelser, dvs bestemmelser som ikke uttrykker noen helhetlig tilnærming til informasjons-/datasikkerhetsområdet.[4]

"Sikkerhet" og "sikring" kan selvsagt også gjelde annet enn informasjon. Sikkerhet kan for eksempel gjelde helse- og miljø, brann- og eksplosjon, trafikk/transport, el-forsyning osv. Selv om slike sikkerhetsspørsmål i utgangspunktet utgjør selvstendige områder, er det viktig å understreke at informasjonssikkerhet er innvevd i disse andre sikkerhetsområdene. Fordi informasjonssystemer styrer sentrale prosesser på nær sagt alle livsområder, vil det ofte være betydeli-

3 "Data" er noe som, når de blir fortolket, gir "informasjon" til brukeren. Informasjon er med andre ord det en kan utlede av data. Fordi data kan fortolkes innenfor mange referanserammer, kan det utledes forskjellig informasjon fra samme data.

4 Se om dette i Dag Wiese Schartums artikkel "Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning", under publisering i Nordisk årbok i rettsinformatikk 2004, Norstedts forlag, 2005.

ge elementer informasjonssikkerhet i alle sikkerhetsområder. Et godt eksempel på dette er forskrift av 16.12.2002 nr 1606 om beredskap i kraftforsyningen, der informasjonssikkerhet er en integrert del av den samlede reguleringen, se kapittel 6 i forskriften.

Når vi bruker "informasjonssikkerhet" er det noen *krav til informasjonen* vi ønsker å sikre. Sikkerhetsbestemmelsene pålegger tiltak som må iverksettes for at disse kravene skal ivaretas. Vi har altså både bestemmelser som stiller (grunnleggende) krav til informasjonen, og bestemmelser som regulerer hva som må gjøres for å sikre at disse kravene skal bli en etterlevet. Lovgivningen stiller for eksempel opp bestemmelser om taushetsplikt, mens sikkerhetsregelverket stiller krav til informasjonsbehandlingen som øker sannsynligheten for at taushetsplikten blir effektiv (passordbeskyttelse, brannmur, loggføring mv). På lignende måte stiller (bl.a) offentlighetsloven opp krav til innsyn i offentlige saksdokumenter, mens sikkerhetsregler stiller krav som øker sannsynligheten for at folk faktisk kan få tilgang til de opplysningene de har krav på å se (krav om reservekopiering, "oppetider" for informasjonssystemet mv).

Vi kan etter dette snakke om et skille i regelverket mellom "grunnregler om informasjon" og "sikkerhetsregler". Grunnreglene er slike som angir primærmålet, dvs at opplysninger ikke skal tilflyte uvedkommende, skal være tilgjengelig for de som har lovlig tilgang og ikke skal kunne endres på uautoriserte måter. Sikkerhetsreglene er regler som skal støtte opp om og sikre at grunnreglene faktisk blir realiserte.

I figuren er sikkerhetsreglene angitt ved hjelp av tre "soner". Sonene er ment å angi ulike grader av intensitet i sikkerhetsreguleringene. I den innerste sonen har vi de systematiske og helhetlige reguleringene av informasjonssikkerhet, jf ovenfor. Personopplysningsforskriften, E-forvaltningsforskriften, IKT-forskriften og informasjonssikkerhetsforskriften er eksempler på slike regelverk. Denne typen regelverk angir samtidig tyngdepunktet i de seneste årenes regulering av informasjonssikkerhet.[5]

Midterste sone betegner sikkerhetsregler i form av mer enkeltstående bestemmelser, dvs bestemmelser som løser konkrete problemer, for eksempel som respons på en uheldig hendelse eller lignende.[6] Begge disse kategoriene representerer eksplisitt regulering av informasjonssikkerhet, fordi kravet om

5 Se Dag Wiese Schartums artikkel "Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning", under publisering i Nordisk årbok i rettsinformatikk 2004, Norstedts forlag, 2005.

6 Se for eksempel forskrifter av 25.02.2000 nr 298 om Den norske kirkes medlemsregister, som i § 10 regulerer datakvalitet og tilgjengelighet, samt fastsetter regler om varsling av Datatilsynet i tilfellet av datainnbrudd.

sikring går direkte frem av rettsreglene. I ytterste sone av figuren finner vi imidlertid "implisitt" regulering av sikkerhet, dvs der det ikke sies i klartekst at sikkerhetstiltak skal treffes, men hvor dette følger indirekte av regler i lov eller forskrift eller av uskrevne rettslige prinsipper. Det viktigste eksempelet på siste kategori er grunnregler i kombinasjon med internkontrollbestemmelser, dvs bestemmelser som pålegger rettssubjektene å vurdere om det er behov for å iverksette tiltak for å sikre etterlevelse av rettsregler for øvrig. Kombinasjonen av internkontrollbestemmelser og grunnregler som stiller krav til konfidensialitet, integritet og tilgjengelighet, kan med andre ord ses på som sikkerhetsbestemmelser. På lignende måte kan for eksempel prinsippet om forsvarlig saksbehandling i kombinasjon med regler som gir krav på tilgang til informasjon, innebære en forpliktelse til å iverksette tiltak for å sikre slik tilgang. Etter offentlighetsloven bestemmer forvaltningsorganet innenfor rammene av krav til forsvarlig saksbehandling hvorledes gjennomføringen av innsyn skal skje. Dersom krav til forsvarlig saksbehandling tilsier det, må de med andre ord treffe tiltak som sikrer tilgjengeligheten.

Denne tredelingen av feltet informasjonssikkerhet, viser både noe om mangfoldigheten av den relevante rettslige reguleringen, og omfanget av de reguleringer som med rimelig grunn kan hevdes å være del av den familie av rettsregler som vi kan si gjelder informasjonssikkerhet. I et videre arbeid med sikte på å forbedre den rettslig regulering av informasjonssikkerhet, er det neppe hensiktsmessig å oppta seg med alle tre "soner". Etter mitt syn er det – i alle fall initialt – grunn til å legge avgjørende vekt på de helhetlige informasjonssikkerhetsregelverkene. Først etter at hovedspørsmålene knyttet til denne gruppen rettsregler er tilfredsstillende behandlet, bør en (i særlig grad) befatte seg med andre typer regulering av informasjonssikkerhet. Det er dessuten grunn til å anta, at et vellykket arbeid med kjernen av regelverk vedrørende informasjonssikkerhet, også vil kunne ha positive effekter for øvrig relevant regelverk.

Dersom vi ser på de grunnreglene om informasjon som bestemmelser om informasjonssikkerhet skal ivareta etterlevelsen av, er dette et konvensjonelt krav vedrørende konfidensialitet, integritet og tilgjengelighet. En kan imidlertid tenke seg sikkerhetsregler som skal ivareta etterlevelsen av flere andre grunnregler; for eksempel regler om informasjonskvalitet, entydig identifisering av personer/virksomheter/objekter som det er knyttet informasjon til, autentisering av personer som gjør bruk av informasjonssystemer og annet. Hva som tas med når informasjonssikkerhet skal ivaretas, er dels et spørsmål om konvensjon, dels et spørsmål om hensiktsmessighet. I norsk regelverk finnes det eksempler på bestemmelser som går videre enn det som er vanlig for informasjonssikkerhet. I helseregisterloven er det for eksempel tatt inn en bestem-

melse i § 16 om " Sikring av konfidensialitet, integritet, *kvalitet* og tilgjengelighet" (min kursiv).[7] En helhetlig tilnærming til informasjonsbehandling kan tilsi at dette er en hensiktsmessig løsning. Dersom en imidlertid ser på hva slags kompetanse som kreves for å ivareta de ulike elementene i kravene til sikring, kan det være en kommer til motsatt resultat. Sikring av konfidensialitet, integritet og tilgjengelighet er i stor grad noe som kan sikres gjennom fysiske, tekniske og teknologiske tiltak, og i tillegg "organisatoriske" tiltak vedrørende systemarkitektur, konfigurering av systemet mv. Slike spørsmål kan håndteres av "teknologer", og disse spørsmålene oppstår i tilknytning til ethvert informasjonssystem. Derfor er dette "globale" informasjonssikkerhetsspørsmål.

Når det gjelder kravene til opplysningskvalitet, trenger en ofte en helt annen type kompetanse. For å vurdere om opplysninger er relevante, fullstendige og korrekte mv, må vurderingen skje innen spesifikke faglige rammer og i forhold til bruksformålet. Opplysningskvalitet i helsesektoren er med andre ord et medisinsk-faglig spørsmål, i offentlig forvaltning er det ofte et forvaltningsrettslig spørsmål, og innen anleggsbransjen er det kanskje et ingeniør-faglig spørsmål. Slike sikkerhetsspørsmål er ikke "globale" men fagspesifikke; dvs de er relevante for informasjonssystemer innen et visst fagområde. Her tar jeg ikke stilling til hvilken systematikk som er mest hensiktsmessig. Poenget er bare å understreke at avgrensingen og kategoriseringen av spørsmål vedrørende informasjonssikkerhet ikke er "naturgitt", men er bl.a. avhengig av en rekke pragmatiske vurderinger.

3 Helhetlig blikk på regelverksarbeid

Det er grunn til å anta at muligheten for vellykket regelstyring øker dersom en utfører et vedvarende og systematisk arbeid. Her vil jeg argumentere for anvendelse av en enkel syklisk tilnærming der regelverket blir til ved hjelp av forarbeider, trer i kraft og anvendes (og det vinnes erfaringer med regelteksten), og deretter blir regelene evaluerte. Evalueringene inngår i et forarbeid som fører til vedtak om regelendring, de nye reglene anvendes osv.

Regelverkssyklusen (figur 2) skal forstås slik at en på hvert av de tre stadiene har som oppgave *å tilrettelegge for det neste trinnet i syklusen*: Forarbeidene legger til rette for regelanvendelse, regelanvendelse legger til rette for evaluering, og evalueringen legger til rette for (nye) forarbeider. Det er dessuten et viktig poeng at den sykliske "bevegelsen" er iterativ ved at den gjentas periodisk så lenge regelverket eksisterer. Hvor hyppige og langvarige periodene bør være, er et hensiktsmessighetsspørsmål som må vurderes konkret.

7 Et annet eksempel er forskrift om Den norske kirkes medlemsregister, se forrige fotnote.

Det neste enkle poenget med regelverkssyklusen, er at det på hvert av de tre stadiene må forventes en viss form for virkemiddelbruk, dvs det må treffes tiltak som er egnet til å gjøre arbeidet i hvert trinn så godt som mulig. Her vil jeg spesielt trekke frem virkemidlene:

- organisering,
- metodikk og
- verktøy.

Sett i sammenheng med det som er sagt ovenfor, betyr de nevnte virkemiddeltypene at målet må være å sette inn slike virkemidler som er egnet til å tilrettelegge for neste stadium av arbeidet. Spørsmålet blir dermed (bl.a.) hvilke organisatoriske tiltak under forarbeidene er egnet til å lette regelanvendelsen? Hvilke metodikker under regelanvendelsen er egnet til å lette evalueringen? [osv] I dette notatet har jeg bare anledning til å redegjøre for enkelte aktuelle virkemidler. Nedenfor vil jeg derfor si noe om mulige samordningsmetoder knyttet til forarbeidet (avsnitt 6), elementer av verktøy fordelt på alle tre trinn i syklusen (avsnitt 7), og til slutt litt om organisering av regelanvendelsen (avsnitt 8).

4 Motsatte perspektiver på regelstyring av informasjonssikkerhet

Et helt grunnleggende spørsmål er *hvorfor* vi skal introdusere og/eller forbedre regelverk om informasjonssikkerhet. Her vil jeg velge et enkelt og kanskje litt retorisk grep ved å spørre om det er effektiv styring eller "brukervennlig" regelverk vi vil ha? Dette er selvsagt en for enkel og firkantet problemstilling, men den er etter min mening nyttig for å identifisere noen mulige motsetningsforhold som det kan være en utfordring å håndtere når informasjonssikkerhetsregelverk skal etableres eller endres. Et innledende poeng er i alle fall at det neppe er grunn til å anlegge en snill harmonimodell der alle gode ønsker settes side ved side uten å undersøke i hvilken grad det er mulighet for konflikter. Mitt utgangspunkt er at det er legitime og gode grunner til både å ønske mer effektiv styring av informasjonssikkerheten *og* til å regulere sikkerhetsspørsmålene på en måte som er i bedre harmoni med de berørte personenes og virksomhetenes ønsker ("brukervennlig"). Poenget er imidlertid at sannsynligheten er stor for at det – i alle fall under visse omstendigheter – er konflikt mellom disse målsettingene. Derfor er det trolig ikke mulig å ta hensyn til begge mål uten å gjøre avveininger og modifikasjoner av utgangspunktene. Dette betyr likevel ikke at det alltid vil være motstridende interesser. Samtidig som det er grunn til å anta at det vil forekomme konflikter, er det grunn til å anta at det vil forekomme interessesammenfall. Konfliktene kan

imidlertid antas å være av størst interesse fordi det er på slike punkter at regelverkets effektivitet settes på den største prøve. Det er derfor i slike spørsmål virkemiddelbruken i "regelverkssyklusen" må være mest intens og overveiet, jf forrige avsnitt.

Jeg forutsetter at informasjonssikkerhetsregelverk må inneholde bestemmelser som gir pålegg om plikter og/eller innskrenking av rettigheter, og at slike regler dessuten vil være ressurskrevende å etterleve for "pliktsubjektene". Dersom denne forutsetningen ikke er oppfylt er det mindre trolig med noe motsetningsforhold av betydning, og resonnementene her vil i så fall være lite relevante.

Et viktig perspektiv på arbeidet med informasjonssikkerhetsregelverk er som nevnt styrings- eller myndighetsperspektivet. Da ser vi spørsmålet om informasjonssikkerhetsregelverk som et spørsmål om hensiktsmessig politisk og rettslig styring, for å nå mål som er fastlagt gjennom det demokratiske styringssystemet. I dette perspektivet er det nærliggende å legge vekt på hva som representerer den mest effektive styringen. Det kan da være at rettsregler om informasjonssikkerhet kan gi effektiv styring alene. En annen mulighet er at regelverk kun gir effektiv styring under visse forutsetninger, og for eksempel i kombinasjon med andre styringsmidler (økonomiske, organisatoriske, pedagogiske mv). I dette perspektivet står det derfor helt sentralt å vurdere hva som – samlet sett – gir den beste styringen mot de fastsatte politiske målene, og regelverk om informasjonssikkerhet kan være ett element. Når en eventuelt velger regelstyring, blir neste spørsmål hvilke krav som må stilles til denne for å oppnå best mulig virkning.

Dersom vi i stedet inntar et "bruker-" eller "virksomhetsperspektiv", dvs setter oss inn i de virksomheters/personers sted som skal forstå og etterleve bestemmelsene, kan de viktige problemstillingene raskt bli andre enn med styringsperspektivet. Selv om "begge sider" langt på vei kan være enige om at det eksisterer et udekket sikkerhetsbehov, kan de tenkes å være uinteresserte i myndighetsregulering fordi de vil stå fritt mht hvorledes sikkerheten bør ivaretas. Det foreligger da ingen målkonflikt, men en virkemiddelkonflikt. Med et slikt utgangspunkt, kan det være at kunnskap om sikkerhetsreglene ikke oppfattes som viktig, og de vil uansett ikke prioritere effektiv styring og effektivt regelverk på området. Sagt med andre ord kan det være at en rekke virksomheter er svært lykkelige over å *ikke* kjenne kravene til sikring av personopplysninger. I den grad rettsreglene blir kjent og blir forsøkt etterlevet, vil det være viktig for de aktuelle virksomhetene at reglene har et innhold som i så stor grad som mulig er tilpasset deres virksomhet, at bestemmelsene er lette å forstå mv.

Selv om det i en viss grad må antas å være sammenfallende interesser mellom myndighets- og virksomhetsperspektivet, er det etter min mening grunn

til også å forutsette at det ofte vil foreligge noen grad av motsetning. Det betyr at myndigheter som ønsker å bedre informasjonssikkerheten ved å gi regelverk, må legge vekt på å identifisere mulige mål- og virkemiddelkonflikter. Slik kunnskap bør brukes for om mulig å *harmonisere* ved å minske selve motsetningsforholdet. Motsetningsforholdet kan trolig reduseres ved å foreslå reguleringer som:

1. har et lite omfang (ekstensivt, intensivt), og
2. lett kan tilpasses den enkelte virksomhet (fleksible krav), og
3. lett kan forstås, og
4. som det er praktisk lett å anvende

Oppfyllelse av kravene i 1) – 3) vil lett innebære at styringsambisjonene må reduseres. I et brukerperspektiv kan oppfyllelse av 4) på den andre siden tenkes å kompensere for manglende oppfyllelse av kravene i 1) – 3). Et omfattende regelverk som det er krevende å fortolke/forstå, kan for eksempel bli mer akseptabelt dersom det følger verktøy med som automatiserer og på annen måte legger til rette for så enkel anvendelse av regelverket som mulig, se avsnitt 7. Ut i fra denne enkle betraktningen kan det derfor antas at kraftige verktøy som gjør det lettest mulig å anvende regelverket, er en av nøklene til å redusere det antatte motsetningsforholdet mellom styringsperspektivet og virksomhetsperspektivet. Gitt et komplekst og vanskelig sikkerhetsregelverk (jf 1 – 3), kan verktøy bli avgjørende for regelverkets effektivitet, dvs for i hvilken grad styringsambisjonen vil bli realisert.

Selv om motsetningsforholdet mellom de to perspektivene ikke kan harmoniseres (jf punktene 1 – 4), kan *betydningen* av dette motsetningsforholdet reduseres. Således kan myndighetene for eksempel tvinge igjennom etterlevelse ved hjelp av kontroller og sanksjoner. En annen mulighet er å bruke positive tiltak, for eksempel ved å gi økonomisk kompensasjon for ressursbruk. Selv om motsetningsforholdet kan reduseres, antar jeg at en slik strategi neppe er særlig aktuell som hovedstrategi, og at en viss grad av harmonisering derfor som oftest vil være et ønskelig element.

5 Kommunikasjon av sikkerhetsregelverk

Utgangspunktet for den følgende diskusjonen er at sikkerhetsregler er uttrykk for ønsket om effektivt å styre sikkerhetskritisk informasjonsbehandling, jf styringsperspektivet i forrige avsnitt. Denne styringen kan være politisk og/eller faglig begrunnet. Her går jeg ikke nærmere inn på spørsmål vedrørende det materielle innholdet av sikkerhetsreglene og de mulige motivene for vedtakelse

av regler. Utgangspunktet er kun at det foreligger en legitim ambisjon om å styre informasjonssikkerhet, og at utforming av regelverk er en betydningsfull del av denne styringen. Spørsmålet blir da hvorledes slike sikkerhetsregler bør utformes for å sikre mest mulig effektiv styring. Det er neppe grunn til å tro at det finnes allmenngyldige svar på et slikt spørsmål, og siktemålet her er derfor kun å peke på relevante "tankeskjemaer", hensyn og tiltak som kan være til hjelp i bestrebelsene for å etablere en effektiv regelstyring. Den følgende diskusjonen kan ses som en ekspansjon og videreutvikling av den enkle listen (med punktene 1 – 4) i forrige avsnitt.

Til grunn for ethvert regelverksarbeid må det antas å ligge en målsetting om å uttrykke et adekvat innhold med høy faglig kvalitet. En slik målsetting kan trekke i retning av å regulere

- mange forhold (ekstensiv regulering)
- hvert forhold på en inngående måte (intensiv regulering)
- hvert saksforhold på en detaljert måte (detaljert regulering)
- hvert saksforhold på en presis måte (presis regulering)

Ekstensiv regulering kan for eksempel invitere til å regulere mange forskjelligartede forhold som kan ha betydning for informasjonssikkerheten. Dersom en følger denne linjen vil "alle" forhold, innen alle virkemiddeltyper inngå i samme regelverk. Det betyr at en regulerer spørsmål om organisering, ansvarsforhold, rettslige forhold (avtaler mv), økonomiske forhold (utgiftsdeling, tvangsmulkt mv), tekniske forhold (vedrørende bygninger, maskiner, programvare mv), pedagogiske forhold (opplæring, informasjon mv) og andre forhold som en måtte mene kan ha innvirkning på sikkerhetsnivået.

I tillegg kan en velge en *intensiv* regulering, dvs at en innen hvert hovedelement i reguleringen også angir mange delelementer. Organisatoriske forhold kan for eksempel reguleres slik at en rekke spørsmål av denne typen blir regulert (hvilke organisatoriske enheter som skal eksistere, hvilke roller som skal inngå i slike enheter, hvorledes personene i rollene skal samarbeide, hvilke prosedyrer som skal eksistere osv). Tilsvarende kan en tenke seg at ethvert forhold i hele bredden av reguleringen (jf den ekstensive dimensjonen) kan reguleres på intensive måter, dvs en velger å angi en rekke krav vedrørende tekniske, rettslige, økonomiske, pedagogiske og eventuelt andre aspekter ved reguleringen.

Hvert enkelt element i dimensjonen ekstensiv/intensiv kan dessuten angis på en *detaljert* måte. Et element innen den delen av regelverket som gjelder organisatoriske forhold, er for eksempel spørsmål om avvikshåndtering. En ikke-detaljert regulering av dette vil for eksempel være å fastsette at "Det skal

eksistere rutiner for avvikshåndtering". En detaljert regulering vil være å fastsette mange krav til hvorledes denne avvikshåndteringen skal være.

Innen hvert regelelement kan det dessuten legges vekt på en høy grad av *presisjon*, dvs slik at det språklige uttrykket blir så entydig som mulig og dermed – i størst mulig grad – eliminerer muligheten for at regelteksten skal leses/fortolkes på annen måte enn intendert fra regelmyndighetens side. Høyt presisjonsnivå kan for eksempel søkes oppnådd ved å innføre legaldefinisjoner ("med avvikshåndtering menes …"), faguttrykk, bruke formaliserte innhold basert på matematikk eller logikk (for eksempel uttrykke risiko ved hjelp av en likning), ved hjelp av tekstoppsett som tydeliggjør rekkefølgen i vurderinger, om vilkår er alternative eller kumulative, og på mange andre måter.

Dersom en velger å gjøre omfattende bruk av alle de fire nevnte muligheter, er det selvsagt en mulighet for at en dermed også har klart å uttrykke dekkende og ideelle krav til informasjonssikkerheten. Det åpenbare problemet er imidlertid at innholdet også skal kommuniseres og iverksettes, og et isolert sett idealtypisk sikkerhetsregelverk kan stå i fare for å ha liten effekt dersom de som skal etterleve regelverket i) ikke forstår det eller ii) ikke har tid, råd eller evner til å iverksette rettsreglene i sin virksomhet. Av disse og andre grunner må det derfor skje en avveining mellom hensynet til "fullstendig regulering" og "effektiv regulering". Hypotesen er her at en "fullstendig regulering" (ekstensiv, intensiv, detaljert og presis regulering) bare vil være effektiv under helt bestemte forutsetninger, og at det derfor ofte bør vurderes å tilpasse reguleringen til hva det faktisk er mulig å kommunisere og iverksette.

Før det skjer en tilpasning, er det grunn til å se nærmere på enkelte forhold som må antas å ha betydning for hvor lett eller vanskelig det vil være å kommunisere innholdet av et regelverket, jf i) ovenfor. Den følgende gjennomgangen er ikke ment å være fullstendig, men antas å omfatte flere forhold som ofte kan være av vesentlige betydning. Jeg kommer ikke her nærmere inn på forhold knyttet til iverksettelsen av regelverk i den enkelte virksomhet, jf ii) ovenfor. Dette vil imidlertid bli nærmere belyst i AFINs prosjekt "Legal Information Security Regulations - An instrumental perspective", som vil bli gjennomført i perioden høsten 2005 – høsten 2007.[8]

Sikkerhetsreglene inngår i "egne" regelverk

En viktig og grunnleggende erkjennelse er at de fleste som forventes å etterleve sikkerhetsregelverk ikke er jurister. Denne enkle kjensgjerningen har flere viktige implikasjoner. En mulig konsekvens er at deres kunnskap om retts-

8 Prosjektet er finansiert av forskningsprogrammet IKT-SoS ved Norges forskningsråd.

forhold primært er knyttet til regelverk som de kjenner som "deres", dvs den særlovgivning som gjelder for det aktuelle virksomhetsområdet. I dette ligger det med andre ord en antakelse om at dersom folk har juridiske kunnskaper, vil denne ofte primært være knyttet til en bestemt særlovgivning. I så fall kan det være grunn til å anta at den mest virkningsfulle måten å kommunisere rettsregler om informasjonssikkerhet på, er å knytte disse til et slikt eksisterende regelverk. Sagt med andre ord, kan det være grunn til å tro at rettsregler om informasjonssikkerhet knyttet til energiproduksjon bør plasseres i eller i medhold av energiloven, at bestemmelser om sikring av personopplysninger i undervisningsinstitusjoner bør knyttes til opplæringsloven og universitets- og høyskoleloven mv.

Av antagelsen ovenfor følger det ikke noen avvising av muligheten for å plassere bestemmelser om informasjonssikkerhet knyttet til eksisterende generell lovgivning dersom denne må antas å være alminnelig kjent. Innen offentlig sektor er for eksempel lovgivningen bygget opp under forutsetning av at berørte personer både kjenner den aktuelle særlovgivningen og felles rettsregler i forvaltningsloven, offentlighetsloven og personopplysningsloven. Antagelsen om at sikkerhetsregler bør inngå i kjente regelverk for å kunne bli godt kommunisert, kan imidlertid uansett være et moment som taler mot rettslig regulering som verken er knyttet til særlovgivning eller til eksisterende, sentral felleslovgivning.

På basis av disse betraktningene, kan det formuleres følgende antagelser om at sikkerhetsregler fortrinnsvis bør plasseres i forhold til følgende prioriterte rekkefølge:

1. Særlovgivning for det aktuelle virksomhetsområdet.
2. Felles, sentral lovgivning.
3. Annen lovgivning, eventuelt ved etablering av nytt regelverk som er uavhengig av 1) og 2).

Det er viktig å presisere at en slik rekkefølge bare gjelder ut i fra nevnte antagelse – isolert sett – og at andre momenter (jf nedenfor) kan endre på den totale vurderingen. Likevel kan det være en rimelig antagelse at det skal helt spesielle forhold til for at løsning 3) skal foretrekkes fremfor løsning 1), og likeledes at det skal klar argumentasjon til for at løsning 2) skal foretrekkes fremfor løsning 1). Av dette følger for eksempel at det skal klare (tilleggs-)argumenter til for å forsvare at regler om sikring av personopplysninger (primært) skal finnes i et felles, sentralt regelverk i stedet for å være en del av relevant særlovgivning. Hensynet til antall regelverk og sikring av likebehandling på tvers av virksom-

hetsområder er blant andre aktuelle argumenter, men jeg går ikke her inn på den konkrete avveiningen.

Regelverket har fellestrekk med kjente reguleringer

Det er også grunn til å tro at regelinnhold best kan kommuniseres dersom det kan inngå som en integrert del av elementer i et eksisterende regelverk, og således bygger på noe den enkelte "regelverkbruker" allerede er kjent med. Dette gjelder særlig dersom "grunnregler om informasjon" og sikkerhetsbestemmelsen kan plasseres i sammenheng, jf avsnitt 2. Tanken er med andre ord at dersom en har et regelverk med bestemmelser om taushetsplikt eller lignende, er muligheten best for vellykket kommunikasjon av relevante sikringsregler, dersom disse knyttes til taushetspliktbestemmelsen. I dette ligger det en antagelse om at "jo nærmere og mer integrert, jo større er muligheten for vellykket kommunikasjon. Dersom loven har en regel om taushetsplikt, vil det da være bedre å sette sikringsbestemmelsen direkte inn i sammenheng med denne bestemmelsen, enn å plassere den i en tilhørende forskrift eller i en annen del av samme lov.

Krever forhåndskunnskaper som adressatene har

En nærliggende antagelse er at det er lettere å kommunisere et regelinnhold på en vellykket måte dersom innholdet korresponderer med den kunnskap og erfaring de personer har som skal etterleve de aktuelle reglene. Dette kan danne grunnlag for å anta at jo mer spesialisert kunnskap som kreves for å forstå og etterleve et regelverk, desto mer usikkert er det om regelinnholdet kan kommuniseres og etterleves på en tilfredsstillende måte. En annen mulig implikasjon, er at en ekstensiv regulering kan gi en mer utfordrende kommunikasjonsoppgave fordi det kan være fare for at den virksomheten som skal etterleve regelverket mangler en tilsvarende bred kompetanse.

Dersom man henvender seg til store virksomheter er det generelt større grunn til å anta at de har eller har mulighet for å ha en viss grad av spesialisering og bredde i organisasjonens samlede kompetanse. I en stor virksomhet vil det for eksempel ofte finnes informasjons- og/eller opplæringskompetanse som har forutsetninger for å forstå og etterleve krav til pedagogiske tiltak mv, de kan ha jurister som har forutsetninger for å etterleve krav til avtaleregulering i tilknytning til utkontraktering, teknologer som forstår seg på tekniske spørsmål vedrørende kryptering, brannmurer o.s.v. Også for større organisasjoner vil krav til brede og/eller spesialiserte kunnskaper innebære en utfordring mht intern ledelse og koordinering.

Hensynet til adressatenes forhåndskunnskaper tilsier for det første at regelverk primært bør utformes ut i fra kunnskap eller kvalifiserte antagelser om hva slags kompetanse de aktuelle virksomhetene typisk besitter eller med rimelige midler kan skaffe seg. Dette kan peke i retning av å utforme regelverk innen bestemte virksomhetsområder (jf spørsmålet om særlovgivning), og/eller ut i fra virksomhetenes størrelse (og dermed mulighet for å skaffe og vedlikeholde bred og/eller spesialisert kompetanse).

Reglene er beskrevet som en arbeidsprosedyre

Det å forstå en regeltekst innebærer å skjønne hvorledes regelmyndigheten ønsker at vi skal forholde oss, fordi etterlevelse av rettsregler innebærer at vi må utføre noen handlinger. Problemet med å omsette ord til handling, handler bl.a. om å forstå hva som er "prosedyren". Regelverk er ofte fragmentarisk ved at det er formulert regelfragmenter som den enkelte regelanvender selv må sette sammen for å forstå hvorledes han skal forholde seg. Anvendelse av et fragmentert regelverk krever imidlertid generell problemforståelse og en viss juridisk kompetanse som en ikke uten videre kan forvente at den enkelte som skal etterleve sikkerhetsbestemmelsene har. Det kan derfor være grunn til eksplisitt å angi en prosedyre, dvs den konkrete fremgangsmåten som må følges for å nå et tilfredsstillende resultat: For den som kan lage sukkerbrød, er det nok å få oppgitt hva ingrediensene skal være og vedkommende vil vite at det må følges en helt spesiell fremgangsmåte for å få et vellykket resultat. Uten denne kunnskapen, er det gode muligheter for et mislykket resultat selv om alle ingredienser er kjent med nøyaktige mål. På lignende måte kan en det være vanskelig å etterleve et sikkerhetsregelverk selv om alle "ingredienser" er kjent, dersom regelverket ikke samtidig er klart vedrørende rekkefølgen på utførelse av de ulike arbeidsstegene som loven gir anvisning på.

Vektlegging av arbeidsprosedyre innebærer en antagelse om at det er størst mulighet for vellykket kommunikasjon av sikkerhetsregelverk, dersom dette legger vekt på tydelige angivelser av tid/rekkefølge og relasjonene mellom de ulike regelelementene. Dette innebærer særlig at rekkefølgen av rettsreglene i størst mulig grad bør følge rekkefølgen ved en etterlevelse av reglene. Uansett bør det i størst mulig grad være tydelige henvisningsstrukturer mellom de ulike regelelementene som angir anbefalt prosedyre for etterlevelse. Dette speiler en antagelse om at regelverk der det er tydelig hvorledes den praktiske etterlevelsen skal skje, vil være lettere å kommunisere enn regelverk der en primært baserer seg på den enkeltes generelle bakgrunnskunnskaper og kompetanse i å anvende rettsregler. Dermed er det imidlertid ikke sagt at det alltid er mulig eller ønskelig å angi hvert steg knyttet til etterlevelsen. Spørsmålet er avhengig

av en totalvurdering, og hensynet til fleksibilitet kan for eksempel tilsi at en er tilbakeholdende med å angi bestemte prosedyrer som skal følges.

6 Samordning av sikkerhetsregelverk

Et av de første spørsmålene en trenger å ta stilling til når en skal gi nye regler om informasjonssikkerhet eller endre på eksisterende regler, er om og i hvilken grad disse reglene skal samordnes med eksisterende regler om informasjonssikkerhet ellers. Samordning kan særlig begrunnes ut i fra to perspektiver:

- Styringsperspektivet: Samordning av regelverk innenfor området informasjonssikkerhet legger til rette for at den totale offentlige styringen blir sammenhengende og konsistent og dermed mer effektiv. Samordning kan legge til rette for samarbeid når det gjelder ulike tilsynsmyndigheters kontroll og håndhevelse av de aktuelle regelverkene.
- Brukerperspektivet: Dersom reglene skal få anvendelse på virksomheter som allerede er underlagt ett eller flere andre sikkerhetsregelverk, kan hensynet til virksomhetenes økonomi og evne til å etterleve den samlede rettslige reguleringen, tilsi at det gjennomføres samordningstiltak for å gjøre reguleringen så billig og enkel å etterleve som mulig.

Det kan også være ulemper knyttet til samordning. Dette gjelder særlig faren for manglende fleksibilitet i den politiske/faglige styringen ved hjelp av regelverket. Dersom behov for regelendring er begrunnet i behov knyttet til ett virksomhetsområde, mens det innen andre virksomhetsområder ikke eksisterer tilsvarende behov, kan en stå overfor valget mellom å bryte ut av samordningstilnærmingen, gi regler som har uønskede konsekvenser eller å la være å gi regler og tåle følgene av slik passivitet. Sikkerhetsforskriftene til SIS-loven er f.eks. nesten identisk med sikkerhetsbestemmelsene i personopplysningsforskriften kapittel 2. Det er rimelig å tro at denne likheten kan være et argument i seg selv, og at det kan føre til at terskelen mot å endre SIS-bestemmelsene blir høyere, eventuelt at en er forsiktig med å endre personopplysningsforskriften fordi dette vil kunne igangsette parallelle forskriftsarbeider også på andre felt.

Jeg skal ikke her gå nærmere inn på en argumentasjon for eller i mot samordning av sikkerhetsregelverk. Før en slik vurdering kan skje, er det uansett grunn til å undersøke noe nærmere hva "samordning" kan tenkes å innebære. Nærmere analyse viser at begrepet samordning ikke gir noen klare svar i seg selv, og at det er en rekke mulige samordningstiltak å velge mellom. I det følgende vil jeg kort gjennomgå noen hovedalternativer. Alternativene er hentet

fra min artikkel " Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning".[9] I artikkelen blir mulige samordningsteknikker identifisert og supplert med utgangspunkt i det sentrale norske sikkerhetsregelverket.

Felles regler. Et av de sterkeste samordningsmidlene er å introdusere felles regler for informasjonssikkerhet. Kategorien "felles regler" er ment å betegne regler som gjelder for alle samfunnssektorer (eller i alle fall et lite antall brede sektorer), og som regulerer alle eller et stort antall aspekter ved sikkerhetsarbeidet. Dersom et regelverk er gitt anvendelse for bestemte sektorer og aspekter, kan det være grunn til å se på disse som "særregler". Felles regler betegner med andre ord den ene enden av et kontinuum som spenner fra én monolittisk regulering i den ene enden, til mange særregler i den andre enden. Det norske forsøket på å etablere en felles lov om informasjonssikkerhet er et eksempel på en ambisjon om en nærmest monolittisk regulering. Felles regler innebærer mange rettsanvendere innen mange virksomhetsområder, og det kan derfor være et stort problem å sikre en enhetlig forståelse av de felles bestemmelsene. Det kan også være en betydelig utfordring at endringer av felles regler har så mange og uensartede implikasjoner at det kan oppstå rigiditet og vegring mot å gjøre regelendringer, jf ovenfor.

Like regler. Jeg lar "like regler" betegne en strategi der ulike regelverk er identiske eller nær identiske med hverandre. Kapittelet om informasjonssikkerhet i SIS-forskriften er et eksempel på dette. Forskjellen fra "felles regler" (jf ovenfor) er at en ved anvendelse av "like regler" setter identiske regelverk inn i ulike rettslige og teknologiske kontekster, noe som innebærer en aksept for og en forventning om at praktiseringen av reglene kan bli farget av det virksomhetsområdet de anvendes i. En fordel med en slik tilnærming, kan være at fagmiljøene ser på reglene som "sine", samtidig som det skjer en samordning. En ulempe er åpenbart at samordningseffekten vil bli mindre etter hvert som de forskjellige gruppene av rettsanvendere setter preg på forståelsen av bestemmelsene. Ulikheter i rettsanvendelsen vil også kunne gjøre det vanskeligere å holde fast ved like regler etter hvert som det senere skal gjøres regelendringer.

Mønsterregler. "Mønsterregler" betegner en strategi der det utarbeides et regelsett som en antar er gagnlige for mange virksomhetsområder, men der en i utgangspunktet aksepterer og har forventning om at det vil være behov for tilpasninger til de ulike elementene i regelverket. Resultatet blir i så fall regelverk som er like på noen områder, har felles trekk på andre områder og er ulike

9 Artikkelen er under publisering i Nordisk Årbok i rettsinformatikk, Norstedts forlag, 2005.

på atter andre områder. Ulempen med en slik tilnærming er at samordningseffekten kan komme til å bli liten dersom behovet er stort for å gjøre endringer i de mønsterreglene som danner utgangspunktet. Fordelen er selvsagt at en slik tilnærming gir en stor grad av fleksibilitet, samtidig som en viss grad av koordinering sikres.

Bakgrunnsregler. "Bakgrunnsregler" betegner en strategi der et sett av felles regler gjelder i den utstrekning det ikke er gitt særregler. En slik tilnærming kan for eksempel være aktuell dersom en er innforstått med at det finnes så mange særlige behov at særregler er nødvendige, samtidig som en ønsker å begrense mengden av særregler. Forholdet mellom sikkerhetsbestemmelsene i helseregisterforskriftene og bestemmelsene i personopplysningsforskriften, er eksempel på dette. Fordelen er at det blir lettere å unngå mer særregulering enn nødvendig. Et problem kan imidlertid være at det blir vanskelig å bringe på det rene hva den samlede rettstilstanden er, fordi både særregler og de felles bakgrunnsreglene må undersøkes og sammenholdes.

Regelbibliotek. "Regelbibliotek" er betegnelse på en tilnærming som ligner "mønsterregler" og "like regler". Poenget er at en i stedet for å lage hele regelverk (slik kategoriene ovenfor langt på vei forutsetter), har ambisjon om å lage enkeltregler som det vil være bruk for i ulike særreguleringer. For eksempel kan en tenke seg standardiserte regler om organisering av arbeid med informasjonssikkerhet, krav til autentisering mv. I et regelbibliotek er det også mulig å utforme flere varianter av bestemmelser av samme type, for eksempel med forskjellig strenghet i de krav som stilles. Fordelen med en slik strategi er at reglene blir forholdsvis ensartede, og dersom en forutsetter at de utarbeides av regelverkseksperter, vil de også kunne ha en høyere regelteknisk kvalitet enn bestemmelser som formuleres av for eksempel en forskriftsmyndighet. Ulempen er at samordningseffekten kan bli beskjeden, og at det er fare for at det legges for lite vekt på helheten i det regelverk som de "prefabrikkerte" reglene skal inn i.

Felles begrepsapparat. Et særtilfelle av regelbiblioteket er felles begrepsapparat, for eksempel i form av utarbeidelse av felles legaldefinisjoner (av for eksempel "kryptering", "pseudonymisering", "elektronisk signatur" mv.). Regelverk som bruker de samme begreper som byggesteiner, vil få visse felles trekk, og det er grunn til å anta at bruk av felles begreper også kan gi påvirkninger som gir likhetstrekk ut over selve begrepsapparatet.

Felles skjønnskriterier og rettslige standarder. I tillegg til felles begrepsapparat i form av legaldefinisjoner mv, kan det være aktuelt å gjøre bruk av felles kriterier for skjønnsutøvelse eller rettslige standarder ("tilfredsstillende sikkerhet", "akseptabel risiko" mv). At vurderingene er knyttet til de samme kriterier, vil trolig innebære at vurderingene blir mer enhetlige enn om forskjellige

kriterier hadde vært anvendt. Dersom samordningseffekten skal bli merkbar, vil dette imidlertid trolig kreve ytterligere tiltak, for eksempel bruk av felles verktøy eller lignende, jf nedenfor i avsnitt 4.

Opplysende henvisninger. "Opplysende henvisninger" betegner en bevisst bruk av henvisninger til andre regler som må anvendes for å sikre en riktig etterlevelse av en samlet sikkerhetsregulering som er delt mellom ulike regelverk. E-forvaltningsforskriften inneholder slike henvisninger til e-signaturloven og personopplysningsloven, og innebærer at strukturelle og innholdsmessige sammenhenger mellom ulike regelfragmenter gjøres eksplisitte. Fordelen er åpenbart at det kan gi god oversikt. Ulempen er at det kan være vanskelig å identifisere og formidle alle potensielle sammenhenger, og at sammenhenger som blir oversett i praksis ikke vil bli tatt hensyn til.

Felles regelverksarkitektur. Med "regelverksarkitektur" sikter jeg til måten regelverk er bygget opp på, og en felles regelverksarkitektur vil si at regelverkene er konstruert på likeartete måter. Arkitekturen gjelder primært de bærende delene av strukturen, snarere enn innholdet. Felles arkitektur kan for eksempel gjelde felles fordeling av bestemmelser mellom lov- og forskriftsnivået, felles inndeling av regelverk i kapitler, felles rekkefølge på (typer av) bestemmelser osv. Slik felles struktur kan altså tenkes uavhengig av om det er noen form for innholdsmessig samordning. Fremgangsmåten kan gjøre det lettere å orientere seg i ulike regelverk vedrørende informasjonssikkerhet fordi den felles arkitekturen kan skape en felles forventning til hvorledes slike regelverk skal være bygget opp.

I tillegg til de 9 tilnærmingene til bedre samordning av informasjonssikkerhetsregelverk som jeg har nevnt ovenfor, er det flere mulig supplerende strategier som kan lede til bedre sammenheng mellom slike regler. Dette er med andre ord ikke fremgangsmåter som direkte gjelder utformingen av regelteksten, men som omhandler de omgivelser som regelverk om informasjonssikkerhet kan befinne seg i.

Plikt til avviksforklaring er en supplerende strategi. De forskjellige samordningsstrategiene som er nevnt ovenfor kan ha gode grunner for seg. På den annen side kan det konkret være klare motforestillinger til å samordne ved hjelp av de nevnte tilnærmingene. Dersom målsettingen er samordning av regelverk, kan det være grunn til å sikre at visse samordningsstrategier faktisk blir vurdert før de eventuelt blir forkastet. For eksempel kan det være grunn til å kreve at legaldefinisjoner som er introdusert i annet informasjons-sikkerhetsregelverk også blir vurdert når nye likeartete regelverk skal utformes. På samme måte kan det tenkes plikt til å vurdere om et etablert regelverk kan benyttes som "mønsterregler". En slik plikt til å vurdere kan for eksempel være knyttet til en plikt til å grunngi hvorfor en samordningsmåte ikke kan brukes.

På den måten kan en sikre at visse angitte samordningsmuligheter faktisk blir vurdert før de eventuelt blir forkastet.

7 Bruk av verktøy i tilknytning til utarbeiding, anvendelse og evaluering av sikkerhetsregelverk

7.1 Innledning

"Verktøy" betegner her IKT-baserte hjelpemidler av ulike slag. Betegnelsen er upresis men populær, og har etter min mening den fordel at den erfaringsmessig gir en del viktige og riktige assosiasjoner. I figur 3 har jeg forsøkt å illustrere noen aspekter ved verktøy-begrepet slik jeg her bruker det. Ideen er at det grunnleggende verktøyet er et rettslig informasjonssystem, dvs et system som primært inneholder det relevante regelverket. Et slikt system bør trolig – stort sett - være likt for regelmyndigheter og brukere av sikkerhetsreglene, men i figuren har jeg antydet at systemet kan tenkes å eksistere i versjoner for å ivareta særlige behov hos de to aktørene. De firkantede boksene indikerer verktøy som er utformet for å hjelpe myndigheter til å administrere regelverket (venstre boks), og for å hjelpe brukere til å utføre de oppgaver som sikkerhetsregelverket gir anvisning på (høyre boks). I boksene er det indikert hva henholdsvis myndigheter og brukere må gjøre, og disse oppgavene tilsvarer de tre stadiene i "regelverkssyklusen" som er beskrevet i avsnitt 3.[10] Pilene indikerer at prosessene går begge veier: Myndigheter både forbereder/gir reglene i informasjonssystemet og evaluerer dem, brukere både anvender og evaluerer regler. Brukerenes evalueringer/tilbakemeldinger på grunnlag av regelanvendelsen, inngår i myndighetenes evaluering.

Verktøy kan tenkes å bidra til at samordningsmuligheter faktisk blir utnyttet når dette anses å være hensiktsmessig. Verktøyet for myndigheter kan for eksempel inneholde og legge til rette for bruk av bestemte regelverksarkitekturer, legaldefinisjoner, regelbibliotek mv. De kan også legge til rette for tilgang til og analyser av eksisterende regelverk, for eksempel basert på en kategorisering av alle relevante regelverk vedrørende informasjonssikkerhet i henhold til regeltype, forekomster av begreper mv. Slik kan et verktøy legge til rette for å identifisere alle bestemmelser som vedrører sikkerhetsrevisjon eller avvikshåndtering osv. Det er etter min mening grunn til å tro at verktøy ofte vil være en forutsetning for å oppnå reelle samordningsresultater. Årsaken er at

10 I figur 3 har jeg likevel valgt å tydeliggjøre brukerenes deltakelse i evalueringen av regelverk.

samordning ofte er så komplekst og arbeidsintensivt at praktisk tilrettelegging og forsiktig automatisering av støttefunksjoner mv vil være en forutsetning for at det skal skje en tilstrekkelig innsats. Hjelpemidlene kan også gjelde selve regelanvendelsen eller vurderingen av regelverk med tanke på endring og forbedring.

Det er grunn til å understreke at det i verktøyene ikke ligger noen forutsetning om at disse skal uttrykke autorative bestemmelser om hvorledes regelverksarbeidet mv konkret skal skje. I den følgende eksemplifiseringen er poenget at verktøyet innebærer en tilrettelegging som ikke kommer i konflikt med den enkelte regelmyndighets nåværende kompetanse. Det er imidlertid grunn til å tro at felles hjelpemiddel vil virke i retning av en saklig begrunnet og balansert koordinering mellom regelmyndigheter.

7.2 Verktøy for utarbeiding av sikkerhetsregelverk

Et verktøy for utarbeiding og evaluering av sikkerhetsregelverk bør inneholde minst tre elementer:

1. Tilgang til eksisterende sikkerhetsregelverk mv, dvs til et rettslig informasjonssystem.
2. Et "bibliotek" med anvisning på regelverksteknikk, herunder mulige samordningsteknikker med forklaringer og eksempler.
3. Erfaringsmateriale vedrørende sikkerhetsregelverk som skal endres/oppdateres.

Her vil jeg kort gå igjennom noen hovedpunkter til hvert av elementene.

Verktøyet bør for det første inneholde en oppdatert tilgang til alle gjeldende sikkerhetsregelverk. Det kan her være grunn til å skjelne mellom helhetlige reguleringer ("regelverk") og enkeltstående regler som gjelder særskilte aspekter ved informasjonssikkerhet. Når det gjelder sist nevnte kategori bestemmelser, kan det for eksempel være grunn til å gjøre tilgjengelig enkeltregler som ivaretar konfidensialitet for seg, og tilsvarende for regler vedrørende andre aspekter ved informasjonssikkerhet (integritet, tilgjengelighet o.a.). Enhver myndighet som skal utarbeide sikkerhetsregelverk bør med andre ord lett kunne identifisere eksempler på regler som ligner regler de selv planlegger, og dessuten få et grunnlag for å bedømme hvorvidt det er grunn til å ta hensyn til/samordne med annet eksisterende regelverk.

I de aktuelle regelverkene bør en også innarbeide alle eksplisitte henvisningsstrukturer slik at det er lett å studere den sammenheng hvert regelverk/hver enkeltregel står i. Dette gjelder for det første internt i et informasjons-

sikkerhetsregelverk, og for det andre mellom ulike regelverk. I tillegg kan det være ønskelig å tydeliggjøre henvisning til "grunnreglene" så langt som mulig, dvs til de regler som fastsetter de adferdsregler mv som skal sikres. Når SIS-forskriften § 7-11 fastsetter plikt til å sikre konfidensialitet, bør denne bestemmelsen således knyttes opp til alle bestemmelser på området som pålegger konfidensialitet (f.eks. SIS-lovens §§ 12, 13, 14 og 15, samt forskriftens § 7-9).

For det andre bør verktøyet inneholde et bibliotek med diskusjon av forhold som spesielt kan antas å være til hjelp ved utforming av sikkerhetsregelverk. Det er særlig aktuelt med tre typer innhold:

1. Angivelse og diskusjon av momenter vedrørende spørsmål om ekstensiv, intensiv, detaljert og presis regulering, jf avsnitt 5 ovenfor. Diskusjonen bør følges av eksempler på bruk av slike ulike regulatoriske strategier.
2. Angivelse og diskusjon av momenter vedrørende samordning av regelverk og enkeltregler. Også her må teknikkene og dilemmaene eksemplifiseres.
3. Diskusjon av utvalgte råd fra Justisdepartementets hefte "Lovteknikk".

Et verktøy til bruk ved utarbeiding av sikkerhetsregelverk bør for det tredje gjøre tilgjengelig erfaringsmateriale vedrørende det regelverk som skal erstattes eller revideres, dvs materiale som utarbeides i samband med evaluering av tidligere regelverk. Se om dette, nedenfor i avsnitt 7.4.

7.3 Verktøy ved anvendelse av sikkerhetsregelverk

Verktøy for anvendelse av sikkerhetsregelverk bør ses i nøye sammenheng med verktøy for utarbeiding og evaluering av regelverk, jf neste avsnitt. Det er særlig to mulige innretninger et slikt verktøy kan ha; en "tekstrettet" og en "funksjonsrettet". Et tekstrettet verktøy betegner et hjelpemiddel der det primært er regelteksten og supplerende tekster (forklaringer, eksempler og avgjørelser) som utgjør hovedelementet. Et "funksjonsrettet" verktøy er et hjelpemiddel der en søker å støtte opp under etterlevelse av regelverket ved å tilby IKT-baserte funksjoner. Regelteksten vil selvsagt fremdeles være viktig, men det er funksjonene som er mest iøynefallende.

Et tekstrettet verktøy bør inneholde en kommentarstruktur, dvs en samling kommentarer som er knyttet til tekstelementer i regelverket på ulike nivåer.[11] Kommentarene skal sette den enkelte bruker i stand til å lese og forstå de aktuelle rettsreglene. Dette innebærer at det for det første bør være kommentarer som er begrunnet i regelmyndighetens behov for å forklare og presi-

11 Dvs til regelverket som sådan, til kapitler, enkeltbestemmelser, deler av en bestemmelse mv.

sere. Dersom regelverket er en lovtekst, vil de spesielle motivene i odelstingsproposisjonen kunne fungere som kommentarstruktur, eventuelt i redigert og supplert form. For det andre bør det være kommentarer som er utformet ut i fra de spørsmål som har kommet inn fra brukere vedrørende hvorledes regelverket skal forstås, jf neste avsnitt om evaluering. Denne siste delen av kommentarstrukturen skal med andre ord bygges gradvis opp gjennom bruk av verktøyet.

I tillegg til kommentarstrukturen bør det vurderes en parallell *eksempel*-struktur, dvs det bør være eksempler knyttet til utvalgte deler av regelverket der dette anses å være nødvendig eller nyttig for å illustrere konkrete anvendelser av bestemmelser. Eksemplene kan gjerne følge samme mønster som kommentarstrukturen og eventuelt være en integrert del av denne. Det betyr blant annet at enkelte eksemplifiseringer kan gjøres i utgangspunktet, mens supplerende eksempler kan gis som respons på spørsmål som oppstår i tilknytning til bruk av regelverket. Et tredje element kan være å gjøre tilgjengelig autorative avgjørelser vedrørende fortolkning av bestemmelser i regelverket. Særlig er domsavgjørelser og avgjørelser i klagesaker aktuelle.

Et funksjonsrettet verktøy er særpreget ved at det i en viss grad hjelper med å utføre de handlinger som regelverket pålegger eller anbefaler. Dersom det for eksempel skal skje en risikovurdering, vil verktøyet hjelpe med å utføre en slik vurdering ved å gi anvisning – trinn for trinn – på hvorledes en risikovurdering kan skje. Dersom det stilles krav til dokumentasjon, vil et funksjonsrettet verktøy på tilsvarende måte inneholde faste elementer/formater for slik dokumentasjon. Det er selvsagt mange mulige elementer som kan inngå i et slikt verktøy, og ”dynamiske skjemaer” og ”ekspertsystem” er blant de betegnelser som kan passe på mulige løsninger. Jeg kommer ikke her inn på ytterligere muligheter, men nøyer meg med å understreke at et funksjonsrettet verktøy gjør en fullgod tekstforståelse mindre viktig, fordi verktøyet utfører en del av de handlinger som rettsreglene gir anvisning på.

Det er selvsagt ikke slik at tekst- og funksjonsrettede verktøy nødvendigvis er alternativer. Tvert i mot bør et funksjonsrettet verktøy alltid være koplet til tekstrettede moduler. Dette fordi de underliggende rettskildene ikke bør fortrenges av systemløsningen. Tekstrettende verktøy kan imidlertid lettere aksepteres alene. Dersom en har en ekstensiv regulering slik at deler av regelverket forutsetter kunnskap som mange av de som skal følge regelverket ikke kan antas å ha, kan dette være et argument for å legge vekt på å utvikle funksjonsrettet verktøy med høy automatiseringsgrad.

7.4 Verktøy ved evaluering av sikkerhetsregelverk

Det siste elementet i et mulig verktøy, er et hjelpemiddel som legger til rette for systematisk innsamling av erfaringer med praktiseringen av regelverket, på en måte som forbereder evaluering og endring av regelverket. Det er avgjørende at verktøyet for utarbeiding/evaluering står i sammenheng med verktøyet for bruk (jf forrige avsnitt), fordi det er gjennom bruken av regelverket at det skapes situasjoner det er lett å lære noe av på en måte som senere kan benyttes til å forbedre regelverket.

En del av den tidligere omtalte kommentarstrukturen (jf avsnitt 7.3) ble knyttet til spørsmål som fremkommer under bruk av regelverket. Dette forutsetter for det første en funksjon som tillater brukere å formulere og sende inn spørsmål vedrørende fortolkning av bestemmelser. Det er for det andre en forutsetning at det er en myndighet som kan ha et løpende ansvar for å motta, vurdere og svare på innkomne spørsmål. Tanken er at enkelte spørsmål kan danne grunnlag for en forklarende kommentar, eventuelt med et eksempel (jf ovenfor). Andre spørsmål vil ikke bli besvart direkte i form av en kommentar, men inngå i et materiale som anvendes som grunnlag for periodisk evaluering av regelverket. Også de spørsmål som resulterer i løpende kommentarer vil selvsagt inngå som grunnlag for evalueringen.

7.5 Avsluttende bemerkninger om verktøy

Ideelt sett utgjør de tre verktøy som ovenfor er skissert ett integrert hjelpemiddel som dekker hele regelverkets "livssyklus", dvs som kan gi støtte ved utarbeiding av reglene, bruk, evaluering, regelendring, bruk osv. Dette igjen betegner et regelverksarbeid som er basert på en kontinuerlig innsats for på den måten hele tiden å sikre så god kommunikasjon av regelinnhold som mulig, og samtidig stadig gjøre regelendringer som forbedrer kommunikasjon av regelinnhold og som derfor høyner måloppnåelsen, jf avsnitt 3.

8 Organisering av rettsanvendelse

Den siste skissen av virkemiddelbruk på de ulike trinnene i regelverkssyklusen (jf avsnitt 3), gjelder organisering av rettsanvendelsen. Poenget er da at organiseringen av rettsanvendelsen skal tilrettelegge for det neste trinnet, dvs for evalueringen av regelverket. Organisering av rettsanvendelsen ellers vil primært være et spørsmål om å organisere saksbehandlingsarbeidet hos det forvaltningsorganet som har kompetanse på vedkommende fagområde på en måte som gir effektiv ressursbruk, rettsriktige resultater og forsvarlig skjønnsutøvelse. Slike hensyn er åpenbart viktige og legitime, men er knyttet til en-

keltsaksbehandlingen. Organisering av rettsanvendelse og saksbehandling kan imidlertid også skje ut i fra hensynet til evalueringen av regelverket, og slike hensyn kan også være gagnlig i forhold til enkeltsaksbehandlingen.

Tilrettelegging for evaluering kan skje ved å organisere rettsanvendelsen slik at det fremkommer et erfarings- og kunnskapsmateriale som er egnet i den etterfølgende evalueringen. Et synspunkt er at det er for sent å utforme opplegg for evalueringsarbeidet når den aktive evalueringsfasen begynner. Skal en kunne fange opp og forstå de problemer som oppstod da regelverket ble vedtatt og rettsanvendelsen begynte, er det ønskelig med en fortløpende innsamling av materiale som senere kan anvendes i en samlet evaluering.

Et annet synspunkt er at innsamling av erfarings- og kunnskapsmateriale i tilknytning til rettsanvendelsen ikke bør begrenses til forvaltningens saksbehandlere. Ikke minst når det gjelder informasjonssikkerhetsregelverk er rettsanvendere utenfor forvaltningen av stor betydning. Særlig gjelder dette de som i henhold til regelverket skal etterleve bestemmelsene. Rettsanvendelsen bør derfor kunne organiseres slik at den legger til rette for å samle inn materiale fra flere grupper rettsanvendere (saksbehandlere, pliktige personer mv) over hele perioden for rettsanvendelse, dvs fra regelverket trådte i kraft til evalueringsfasen er innledet, jf figur 2 (ovenfor). Et verktøy som det jeg har skissert i avsnitt 7.3 kan ha slike organiserende effekter; Dvs verktøyet blir gjort attraktivt for flest mulige brukere av regelverket, og det legges til rette for fortløpende svar på tolkningsspørsmål mv (noe som kan motivere og øke bruken). Når en når frem til selve evalueringsfasen vil det foreligge et rikt "historisk" materiale. Dette kan suppleres i form av et retrospektivt materiale, dvs materiale som fremkommer ved at en undersøker tidligere saksforhold og begivenheter og spør om hva involverte personer har av hukommelse og oppfatninger.

9 Avsluttende bemerkninger

Etter min mening ligger den mest lovende muligheten for å komme videre i arbeidet med sikkerhetsregelverk i en kombinasjon av systemutvikling og forskning. En eksplorerende tilnærming der en prøver ut idéer og muligheter vil etter min mening lettere skape interesse, entusiasme og resultater enn hva "enda en utredning" vil gjøre.

Jeg tenker meg et opplegg der en gruppe bestående av personer fra regelmyndigheter og akademia spesifiserer krav til et verktøy, dvs krav til et IKT-basert hjelpemiddel for bruk ved håndtering av sikkerhetsregelverk. Et slikt verktøy bør inneholde noen elementer på alle trinn i "regelverkssyklusen" (jf avsnitt 3), og særlig er det grunn til å dekke evalueringstrinnet.

Arbeidet bør starte ved at en arbeider med forholdsvis enkle prototyper som tidlig prøves ut for å vinne erfaringer. På den måten kan en sikre best mulig styring over faglig innhold og økonomi. Dersom det blir utviklet verktøy som regelmyndigheter ønsker å teste, bør slik bruk være gjenstand for forskning, for på den måten å fastslå faktiske effekter av verktøyet, og dermed vinne grunnlag for videreutvikling og videre bruk.

3 ASSESSING E-GOVERNMENT PROGRESS – WHY AND WHAT

Arild Jansen

Research in progress paper

Abstract. The aim of this primarely theoretical paper is to discuss the use of e-government frameworks and benchmarking tools. It is frequently claimed that providing an effective e-government assessment framework is a necessary condition for advancing e-government. However, there are major drawbacks in many of the existing e-government frameworks and surveys, as e.g. lack of a clearly defined purpose, and that they do not allow for specific national contexts and priorities. The paper reviews some of these frameworks and discusses to what extent they really can fulfil their intention in acting as guiding tools in e-government implementations. It is further argued that these different approaches are not likely to provide adequate framework for research that can deepen our understanding in this field.

Key words: E-government, framework, assessment, evaluation, benchmarking,

Introduction

Bench marks was originally used in topography, to mark the spots for intermediate points in a survey of an area. They could be found on a permanent object (e.g. in walls and pillars), as a mark indicating elevation and serving as a reference in topographic surveys and tidal observations. Similarly, framework had to be developed in accurate measurements of the Earth's surfaces; surveying frameworks are erected by measuring the angles and the lengths of the sides of a chain of triangles connecting the points fixed by global positioning. The locations of ground features are then determined in relation to these triangles by less accurate and therefore cheaper methods (Britannica online 2005).

To day, such words have become rather holy in the computerization of the public sector. Various frameworks have been developed to guide the conceptualization and implementation of national e-government programs. Benchmarking departing from these frameworks should help the politicians and other stakeholders to compare their initiatives with similar ones in others

countries, to make sure that their efforts are moving the government in the right direction. Thus, appropriate frameworks are intended to serve two purposes; firstly, to help the development of e-government, secondly, as basis for assessments and evaluations.

In this paper, I will review some of these frameworks and discuss to what extent they really can fulfil their intention in acting as guiding frameworks in the implementation of e-government. I do not question the use of these tools as such. I rather want to discuss to what extent they may really help the politicians and other stakeholders to define the optimal goals and make the best priorities. Could it be so that the strong focus on surveying and ranking of the different nations according to their scores on selected indexes removes the attention from more fundamental issues related to transforming the government by use of ICT? Each nation with its government has its distinct governmental structure, departing from its unique geography, history and culture. Their efforts and initiatives aims at fulfilling the individual goals, taking into consideration their specific national context and priorities. Is it then fruitful to measure their different e-government initiatives and results using standardised indexes? And furthermore, is it feasible to assess and classify national ICT programs according to a common framework?

Perhaps even more important, to what extent can such, rather complex frameworks constitute useful basis for research? In this paper, I will argue that one should rather depart from simpler 'frameworks' or skeletons that allows for many different approaches. The primary strategy for research should be to link studies of e-government efforts to overall national goals and political priorities, taking into consideration their specific democratic and political system, governmental structure and culture etc. Rather than regarding e-government as a separate research area, one should see it as a vast area for a variety of empirical studies, in which one should apply existing scientific knowledge, theories and methodologies from as well IS research as from e.g. organizational studies, political science, etc.

The structure of the paper is as follows. Following this introduction, section two discuss definitions and theoretical frameworks for e-government. In section three are presented some empirical studies and evaluations followed by a discussion of some empirical results.

Theoretical background

E-government is becoming a global phenomenon that is consuming the attention of politicians, policy makers as well as ordinary citizens. A United Nations World Public Sector Report indicated that by 2003, over 173 countries had

developed government web sites. E-government is predicated on leveraging the capabilities and power of ICT to deliver services provided by governments at local, municipal, state and national levels. Beyond service delivery, e-government offers additional channels of interaction among governments, businesses, and citizens, separately or collectively (UN 2003). However, E-government is more than a technological phenomenon. It is transformative in nature, affecting the management of human, technological, and organisational resources processes. Consequently, the implementation of e-government will be a monumental change effort.

What is e-government?

Is it possible to agree upon a common definition of e-government? There exits a number of different definitions of e-government in the literature. Some are rather narrow, focusing on using ICT, particularly the Internet, as e.g. "the use of technology to enhance the access to and delivery of government services to citizens, business partners and employees", (Deloitte Research 2000, p4.) Others view e-government more broadly as efforts to transform government. Such examples can be:

- Electronic information-based services for citizens (e-service) with reinforcement of participatory elements (e-democracy) to achieve objectives of balanced e-government (Bertelsmann Foundation 2001, p4)
- The use of information and communication technologies, particularly Internet, as a tool to achieve better government (OECD, 2003, p 63).
- The use of ICT in public administration combined with organisation changes and new skills in order to improve public services and democratic processes and strengthen support to public policies. COM (2003).
- The use by the government of Web-based Internet applications and other ICTs, combined with processes that implement these technologies, to a) enhance the access to and delivery of government information and services to the public, other agencies, and to government entities; or b) bring about improvements in government to operations that may include effectiveness, efficiencies, service quality, or transformation" (US government 2002)

These definitions may be useful in describing e-government in a broad-based manner, but offer little insight into deeper issues and considerations relating to the construct, and fail to capture the more complex aspects of transforming government or acknowledge the role of the ICT elements. Consequently,

most implementations activities centre on service delivery concerns with little emphasis on real transformation of the services themselves or the processes associated with their delivery (Grant and Chau 2005). They further claim that 'any conceptualization of e-government needs to address a variety of concerns beyond the service delivery elements. Based on a comprehensive literature review, they suggest this definition:

> *"A broad-based transformation initiative, enabled by leveraging the capabilities of information and communication technology; (1) to develop and deliver high quality seamless, and integrated public services; (2) to enable effective constituent relationship management; and (3) to support the economic and social development goals of citizens, businesses and civil society at local, state, national and international level"*
>
> (Grant and Chau, op. cit: p 9).

This definition focus on as well technological as economic, managerial, organisational and social/cultural issues, while the legal issues are not, at least explicitly addressed. To furthermore illustrate the complexity e-government efforts, one should not overlook perspectives as i) e-government as a transformational endeavour, ii) a diverse number of solutions, iii) the relation between e-government, information and ICT, iv) integration, service sophistication and maturity, and v) that it is an international phenomenon which not at least a number of consultant companies world wide are heavily involved in.

E-government: politically or scientifically defined?

However, it is necessary to ask what we actually gain from using such broad and extensive definitions? It seems that these definitions are primarily politically motivated, in that they include all initiatives and activities related to the use of ICT in the public sector, aiming at measuring the magnitude and reach of the specific efforts in various countries. These are, however related to specific goals and priorities, and their value-laden, and accordingly not always commensurable.

In the work on eGovernment in the EU Commission, they focus on these overall objectives (Com 2003):

- A public sector as e.g. *open and transparent*, that is understandable and accountable to the citizens, open to democratic involvement and scrutiny.
- A public sector that is *at the service of all*, being inclusive and exclude no one from its services

- A *productive* public sector that delivers maximum value for taxpayers money

Departing from these clearly defined goals and priorities, I propose a simpler framework, defining basically three distinct groups of stakeholders: *politicians*, *public institutions*, *citizens, businesses and civil society* and thereby distinguishing between 3 different dimensions (e.g. Grønlund 2002): 1) the *democratic* dimension, focussing on the political processes and interaction between the constituents and the government, 2) the *service* dimension which comprises the delivery of all types of electronic services, and 3) the *administrative* dimension including various types of management work, internal routines etc. This may be illustrated in this way:

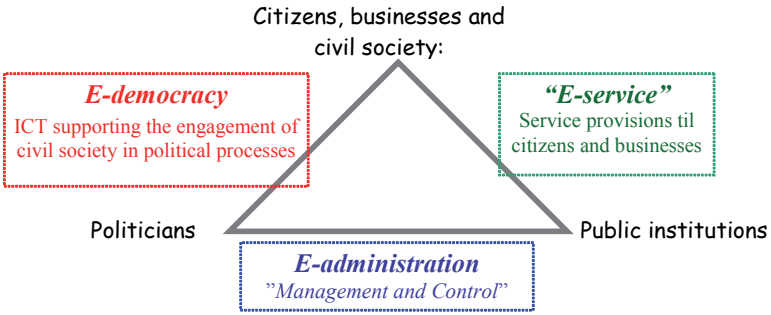


Figure 1: Three major dimension in e-government initiatives

The functions and activities in the different dimension cannot be completely separated, but their focus and priorities is clearly different. And even more important, one cannot use the same theories and models when doing research linked to these different dimensions. Thus, when doing research in each of these areas' we should apply adequate theories and models which we find in well established research fields such as e.g. organisational studies, business administration, and political science. In addition, we need to study the development and maintenance of the different layers of information and organisational infrastructures and back-office routines that is required to support e-government functions, including basic communication and information services, security functions etc.

Assessment and benchmarking of e-government initiatives

Benchmarking of governmental websites and national e-government initiatives has been conducted in a number of years. There are several well-established surveys on e-government (e.g. UN 2002, 2003, 2004, Capgemini2005). These surveys employ different assessment models for e-readiness, digital divide and other relevant factors, leading to varying conclusions on the global state of e-government. The grounds for these efforts are well illustrated by a statement from the EU report (EU, 2001):

> *The ministerial declaration on the eGovernment conference, together with benchmarking survey should give political momentum to the development of online public services and to the identification of the needs for these services at pan-European level. This will have to be complemented by a focus on back-office reorganisation, the creation electronic marketplaces for public procurement and investment in new equipment in administration.*

A survey, conducted by Capgemini on behalf of the European Commission, is part of the benchmarking programme that assesses the progress of eEuropa (Capgemini 2005). The study measures the e-government policy indicator of the eEurope action plan (eEurope 2005). The objective of this action plan "is to develop public services and a dynamic environment for e-business through widespread availability of broadband access at a competitive price and a secure information infrastructure". Thus the eEurope benchmarking indicators are aimed to support member states in achieving the objectives of the action plan.

The council of EU decided that a methodology developed by Capgemini to measure the original indicator in 2001 had to be continued for the scoring of the new indicator. (In the eEurope 2002 Action plan the policy indicator was *"percentage of basic public services availability one line"*, while the new definition is "*number of basic services fully available online*". The EU commission defined a list of 20 basic public services. For 12 of these services, the citizens are the target group while the remaining 8 are targeting the businesses sector. In order to this eEurope 2002 indicator, a four-stage framework (the scoring framework)[1] has been defined[2].

1 E.G. labelled as "The scoring framework", as illustrated in Capgemini's Web based survey on electronic services public services, EU DG Information Society, 2003.

2 See http://europa.eu.int/information_society/eeurope/2005/doc/all_about/online_availability_public_services_-5th_measurement_fv4.PDF

1. Stage 1: Information:
2. Stage 2: One-way Interaction
3. Stage 3: Two-way interaction: The publicly accessible website offers the possibility an electronic intake with an official electronic form to start the procedure to obtain this service. This implies that there must be a form of authentication of the person (physical or juridical) requesting the service in order to reach stage 3.
4. Stage 4: Full electronic case handling: The publicly accessible website offers the possibility to completely treat the public service via the website, including decision and delivery. No other formal procedure is necessary for the applicant via "paperwork".

Based on this evaluation scheme, all old and new member countries have been measured. In the report from the fifth measurement was that the overall average score was 65%, which means that it is located between stage 2 (one-way interaction) and stage 3 (two-way interaction). However, the old 15+[3] member scored 72%, while the10 newcomers achieved corresponding 53%, indicating that these countries are lagging about 2 years behind the old ones.

However, what do us really get from these statistics? In an analysis of these results, it was found that some countries appeared to rather remarkable progress on the last evaluations (e.g. Austria), which have put priorities in improving services that contributed to better ranking (ECEG 2005), while others (e.g. Belgium) had seemingly far less progress, because they had focussed on infrastructural efforts, in particular a national wide citizen security card (Snijkers 2005). It can therefore be argued that this type of one-dimensional framework do not capture the different dimensions of a more advanced public web sites.

In the report, Capgemini states that "the survey only analyses the result of the eGovernment efforts from the perspective of online availability of public services. The results should be integrated into a broader perspective of various eGovernment measures: linking services availability, channel selection, back-office fulfilment capability; and service usage and impact of eGovernment". And even more important: "Initiatives developed by government to enhance the quality of their service provision – service integration, from the pull to push service delivery – are not validated in the indicator, but the information provided by the member states concerning concrete cases is covered in this report." (Capgemini 2005) This is in my opinion fundamental issues in the

3 15+ means the old 15 member countries + Iceland, Norway and Switzerland

discussions on the development of e-government, both in a political and scientific context.

Some experiences from quality evaluations in Norway

The Norwegian government initiated a project together with the research institute Vestforsk[4] to develop a set of quality criteria for evaluating public websites in Norway. The first work started in 2001 and resulted in a set of 21 indicators (Ølnes 2001, 2003). The work has been repeated in the following years, and new set of indicators were developed. The 2004 evaluation was based on an indicator set consisting of 25 items; again some indicators were new, divided in three groups: accessibility, usability and useful services. In all more than 700 public web sites were evaluated (Kvalitet 2005).

A direct comparison between the results in 2001 and 2003 is not possible due to the different indicator sets. However, for the indicators being unchanged from 2001 to 2003 we saw an improvement of more than 10 %. From 2003 to 2004 there have been some improvements (exact figures are not available yet). After the first set of evaluations in 2001 the project group received a lot of feedback, especially from the municipalities, many of them asking for new evaluations since they had changed made changes to their web sites following the evaluation. As such, these evaluations stimulated improvement work, in particular to increase accessibility, but were not very helpful in guiding the development work itself.

How consistent are different evaluation frameworks?

It can be argued, however that such evaluation do only provide us with limited insight of how the websites really are perceived by different people. In parallel with this evaluation, the Norwegian Consumer Council carried out a similar evaluation, however based a different set of indicators (FR 2004). The results from this evaluation differs substantially from the ones conducted by Norge.no, due to that these two indicator sets emphasize different aspects and criteria. It is however, not obvious whether it is the former or the latter of these evaluations that provide the best evaluations. It depends on what aspects you would like to put emphasize on.

In a recent study, a new framework was developed, building on experiences from others (Eikeland and Kongshaug 2005). It was tested on a number of experts. The results showed that the experts interpreted the framework somewhat differently. This illustrates the problems with the results of such evaluation. If not based on very standardised and simple criteria, the results

4 Vestforsk is short for Western Norway Research Institute

are likely to be depending on the evaluators' background, knowledge and preferences. There exist several methods and techniques to improve the value of measurements and evaluations. Nevertheless, all types of evaluations do only measure what is measurable, leaving other aspects out. They are accordingly useful only to a limited extent.

Assessing the E-democracy dimension

Quite another approach was applied in a study conducted by the University of Oslo in 2003 on how Norwegian local and regional municipalities were using their websites to provide information and get feedback from its citizens (Haug 2003). 435 different municipal web-pages were visited[5], with nearly 120 different items for each website. The large database was later supplemented by statistical data describing each municipality, e.g. economic data, size, citizens with access to Internet, etc. The focal point was primarily on to what extent the local municipal websites were used to facilitate what we labelled "political communication". The findings of the study showed that there was large variety in how the municipalities actually were utilizing ICT and Internet for political communication. In general, their web-sites are mostly used for information provision, primarily supporting enlightened understanding, while interaction, supporting effective participation is less frequently available.

The analysis showed, however, that the applied model can only partly explain the variation across the municipalities. It is therefore important to develop more adequate models and thus offer validated knowledge as basis for practical action, e. g. by identifying factors that seem critical for successful application of Internet for stimulating democratic processes. One conclusion from the study was that in order to collect empirical data that can have stronger explanation power, one need to get access to more specific data about the individual municipalities, e.g. by interviewing key persons about their strategies and background for their decision regarding developing the web-sites. It seems clear that the variety in e-democracy initiatives have to be analyzed by using different models than when evaluating e-service implementations. This is clearly demonstrated in e.g. (Hacker and van Dijk 2000)

5 The Internet-based examination of all municipality websites in Norway was conducted by Harald Baldersheim, Morten Øgård et al at Department of Political Science, University of Oslo.

Determining Progress towards e-Government

In an interesting paper Adegboyega, Janowski and Estevez (2005) presents a comparative study of 11 international surveys on e-government between 2001 and 2004. It identifies a common set of 'core indicators' for assessing e-readiness and suggests ways to determine the weights for them. The paper also introduces the concept of a 'target e-ready state' and examines how it may provide a scale for determining the progress of individual countries.

The paper claims that providing an effective e-government readiness assessment framework is a necessary condition for advancing e-government. This framework should not rely solely on the general e-readiness measures, as clearly e-readiness transcends e-government. In fact, one of the major drawbacks of the past e-readiness surveys is lack of a clearly defined purpose, beyond the operational definitions provided. They claim that a framework for effective e-government assessment must instead identify and focus on the critical variables for e-government and consider the peculiarities of the environment assessed.

The paper presents a comparative analysis of the survey series consistently carried out by three organizations between 2001 and 2004: United Nations Department of Economic and Social Affairs (UN-DESA), Accenture, and the Centre for Public Policy of the Brown University. The surveys benchmark countries based on different sets of indicators. For instance, UN-DESA provides information on the maturity of online presence, availability of the basic ICT infrastructure, and human development of UN member states. Accenture examines the breadth and depth (sophistication) of online services of a number of selected countries. The analysis reveals that the use of different sets of indicators and different weights assigned to them lead to varying conclusions on the performance of the countries in terms of e-readiness and e-government.

The conclusion of their study is that the disparity and lack of standards for e-government assessment lead to varying conclusions on the global e-government readiness. It shows that the outcomes from the three e-government surveys do not in general agree on the relative readiness of countries. To aid the provision of standards in e-government assessment, they identified the set of core indicators that are central to e-government readiness, based on the data provided through the 2004 UN-DESA survey. Furthermore, they suggest an approach for determining weights for these indicators, which they believe can serve as a foundation for developing international e-government readiness assessment models.

I believe we all can agree upon that assessing the progress in e-readiness is important for the politicians in each country; in order to get a better understanding of how prepared the citizens are for e-government development

efforts. Statistics on variables as quality and accessibility of the ICT infrastructure, basic skill and competence in the population important data in the planning and implementation work. But a well functioning a-government will rely on well informed, knowledgeable and critical citizens, which cannot be assessed by standardised measure. And furthermore, to what extent it is fruitful to compare such statistics across countries is not at all fully documented, as it is necessary to understand the specific character of the administrative and democratic system in each country.

Use of frameworks in e-government developments

The drive to implement e-government has resulted in the adoption of many e-government visions and strategic and strategic agendas, driven by its own set of social, political and economic factors and requirements (Accenture 2004). Consequently, the missions and objectives that emanate from these e-government visions variously manifest strong focus on selected elements. While some governments' strategic agendas focus primarily on service delivery issues, others may focus more on creating internally efficient systems and processing. Still others may adopt a more comprehensive view, incorporating issues as constituent relationship management and e-democracy. Although each of these view of e-government may be legitimate, there is frequently expressed a need for some common understanding to allow for assessment, comparison and explanation of current efforts to vis-à-vis past and future investments in the e-government enterprise, and on increasing cross functional efficiencies (Grant and Chau 2005).

The literature describes a number of frameworks that in various ways conceptualises e-government development and implementation, see Grønlund (2002), Bertelsmann (2001), Accenture (2004) etc. The most comprehensive model so far (to my knowledge) is developed by Grant and Chau (2005), basing their work on a survey of a large number of previous efforts. Even if their framework does not include all dimensions and aspects of e-government, it may very well illustrate the complexity of such generic models.

Their goal when developing this framework was to characterise and identify the different directions and dimensions of different e-government approaches, and that could be used to "categorize, classify and compare electronic visions, strategic agendas and application initiatives". Furthermore, they want to provide a framework that "should act as a lens to focus attention and awareness on underlying issues and elements that could be debated, discussed and further developed". Their model is outlined in this way:

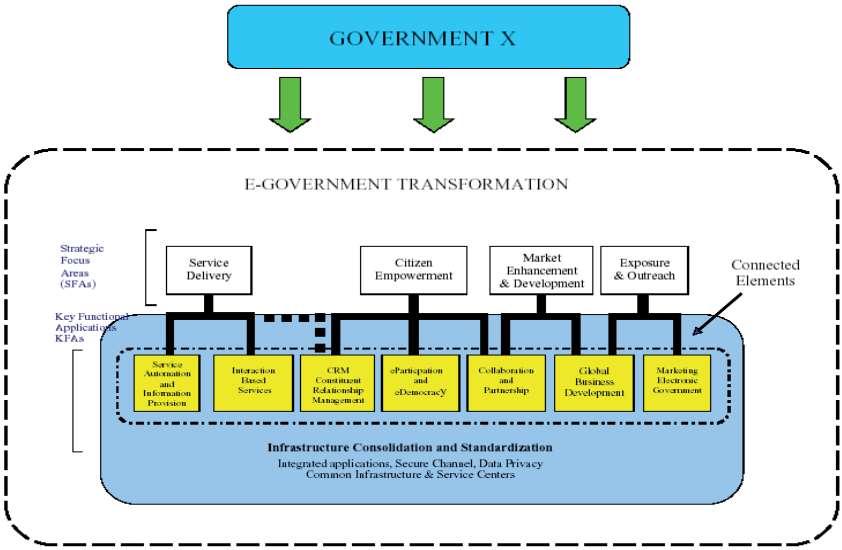


Figure 2: A generic framework for electronic government (from Grant and Chau 2005, p 13)

Grant and Chau have applied there framework on case studies, and finding that framework provided:

- A mapping of diverse electronic government elements to a common perspective
- the ability to compare and differentiate underlying goals and themes between different implementations
- the ability to draw general conclusions and compare differences and similarities across implementations

This framework demonstrates an impressive effort in modelling complex factors and relationships, and that it can be used for assessing and classifying different e-government initiatives. It illustrates the large variety of areas and elements that such frameworks have to include in order to be applicable across different nations and cultures. This framework has also been used in a small study of a Norwegian state agency (Berg, Refsdal and Holmen 2005), but it turned out that it provided only limited usefulness for their study. And more fundamentally, the framework seems primarily to be useful for descriptions and classifications, but not for exploring and explaining why and where.

However, what is interesting with this framework is the emphasis on i) "to enable identification of e-government goals and objectives and ii) be adaptable to country-specific requirements". Every nation has its own functional, social and administrative objects to fulfil. Therefore, every e-government program should be viewed and assessed with respect to its context of applications. A greater understanding of motivation and resulting patterns of development in different settings can facilitate the process of comparing approaches and provide a rational means of setting the reform of public administration on course for efficiency and transparency, with clear orientation towards its citizens (Bertelsmann, 2001). It is vitally important to distinguish patterns of development and motivation for e-government and identify transferable elements. Thus, Grant and Chau (op. cit) point to that e-government development and maturity must reflect the changes in the political, social and economic orientation of the hosting nation. New technology and improved organisational infrastructure will need to be developed to meet such requirements.

Discussions - what type of framework do we need?

The aim of this work has been to review some recent work in this field, and by that to illustrate the large variety of different approaches to modelling and assessing e-governments initiatives. It has been argued that these different approaches are not likely to provide a comprehensive and unifying framework as basis for assessing, classifying and comparing different e-government programs, even though some of the referred work has shown interesting result. These rather complex frameworks may help in providing useful external descriptions, but they will no be able to take into account the specific context of each country. The many different perspectives and interests involved in a national ICT programs may be partly conflicting, and thus require difficult political priorities and considerations, as e.g. efficiency versus quality of services and citizens participation. This is not taken in account in e.g. the scoring framework. Furthermore, it is hard to se how these frameworks can account for national differences in legislation and other regulations.

We have also seen that international surveys and ranking can result in that some countries give priorities to achieve short terms results rather than to gain long effects. This may in particular delay the building of adequate infrastructures and prevent the provision of adequate security and vulnerability measures. Furthermore, in conducting these various measurements and evaluations there will always be great challenges related to reliability and validity of the data collected.

I believe that Grant and Chau's framework presented above can be useful for politicians and other stakeholders on a policy level in the planning and implementation work. But it is not evident that the framework is as useful for doing research. I will therefore argue that we may benefit from using rather simpler "framework" or skeleton, based on the dimensions illustrated in figure 1. We should thus basically distinguish between these three distinct perspectives; corresponding to e.g. Grønlund (2002):

I: The democratic dimension (e-democracy)

The variables associated with this dimension should aim at measuring to what extent ICT-based functions and facilities really support the democratic ideals of a municipality or state agency. Such values are *openness and transparency*, services that are *understandable* and *accountable* to the citizens, open to democratic *involvement* and *scrutiny,* and stimulates *interaction and participation*. Thus, e-democracy studies should not only address services and facilities that my help the interaction between the civil society and the political system, it is important to study whether all types of e-government services and functions support democratic processes.

An example of this type of research is found in Haug (2003), Haug and Jansen (2004) presented above. This study revealed that there is large variety in how Norwegian municipalities actually are utilizing Internet for political communication, but that the models used in the analysis were not able to explain this variation. More adequate theoretical approaches are thus required,

II: The service provision dimension (e-service)

The variables belonging to this dimension should aim at measuring to what extent public electronic services meet all the requirement defined, both related to functionality, quality, user friendliness, security, etc. The scoring framework discussed above will be one possible approach in describing some important qualities of the services. But one major weakness is that this framework is of little help in explaining why and what. Such studies will have to borrow theories from many different research fields, as e.g. information systems, organisational studies etc.

The quality of governmental services or functions cannot fully be measured by a general, context-free evaluation framework or index, but rather has to be evaluated according to different criteria, depending on its context, primary goal and type of users.

III: Efficiency and efficacy dimension (e-administration)

The *efficiency dimension* should focus on the range, content and quality of interaction and cooperation between offices internally) and between different public agencies, both on a state level and on local (municipal) level. This corresponds partly to the horizontal integration indicator discussed above, including organisation transformations. However, it is important to make sure that such studies go beyond measuring effects and consequences, in that they focus on conditions for the different initiatives and efforts, as well as the relation between them.

The arguments for selecting emphasizing distinct dimensions is that

1. They represent three different set of goals and priorities for a nation, and these goals may be both unifying and conflicting
2. The distinction between them combine simplicity and generality, in that they allows for a large range and theoretical and methodological approaches
3. They should be useful for as well research as development work and evaluations, but indifferent ways.

However, these arguments are mainly theoretical, supported by a limited number of empirical studies. Is necessary to review and categorise a lot more of e-government studies.

Infrastructural and organizational aspects

A majority of the research in this field has focused on front-office services; it seems so far to have been less attention on how government need to reorganise in order to meet the challenges and opportunities represented by Internet.

In a study of back office reorganisation[6] it is claimed that there is a strong link between reorganising government back office and electronic public services experiences by users. This is not surprising, as almost exactly the same conclusion have been drawn from the first phase of the "dot.com" wave in which enterprises went on Internet without changing its internal business organisation.

The back-office functions may be organised in different ways to serve a variety of different user services, spanning from simple interaction services

6 The study "Reorganisation of Government Back Offices for Better Electronic Public Services" was conducted by Danish Technological Institute, Copenhagen and Institute for Information management, Bremen and reported to EU in January 2004.

to fulfilled case handling and interaction between different governmental organisation, implying both vertical and horizontal integration, and including both centralised and decentralised solutions. The different elements may be illustrated in this way:

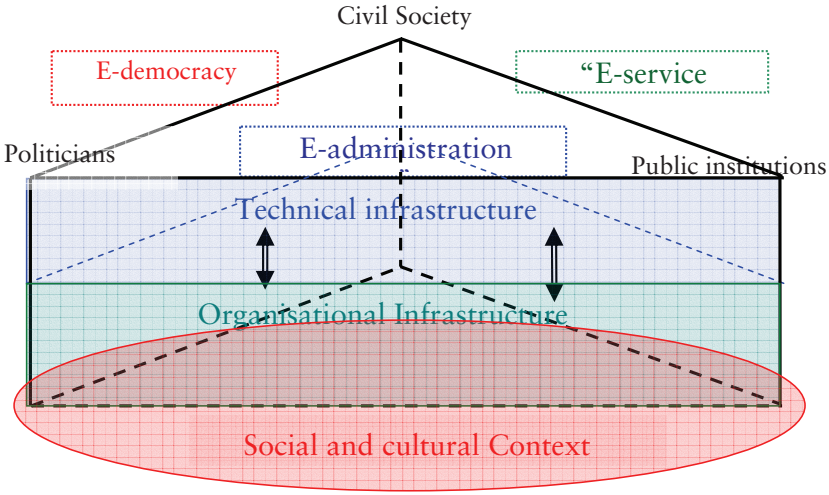


Figure 3: E–government infrastructure - layered architecture

However, the back-office organisation should be seen as an integral part of national infrastructure supporting e-government services and facilities in general. The infrastructure should be understood in a broad sense, including technical, informational and organisational elements, as e.g.

1. an *flexible, secure and reliable* technical infrastructure, that is the network and basic system services
2. the availability of *sufficient information resources* as e.g. databases and other types of information system and applications
3. A well functioning *organisational infrastructure*, which is a back-office organisation that can serve the web site in an adequate way.

However, these requirements do only apply to the supply side. An essential precondition is that the society at large is able to benefit from this e-government structure. Thus, we have to create a necessary social and cultural basis among

the citizens, and the whole civil society. We require a public sector that is *at the service of all*, being inclusive and not exclude anyone from its services.

Conclusions –a extended research agenda is needed

The limited literature review has shown that there exist a number of different approaches to defining framework for e-government assessment and evaluations, many of them having various weaknesses. Rather than to develop standardised framework for assessment and evaluations, one should aim at developing research models that are useful for understanding and explaining the differences in the various nation's implementations of e-governments solutions, linked to their specific national context and priorities. In stead of regarding E-government as a separate research field, one should see it as a vast area for both theoretical and empirical studies, offering a broad range of applications and organizational settings. In such studies, we may apply adequate theories and methodologies from a large number of research fields.

A simple research skeleton has been proposed, including three distinct dimension e-democracy, e-service and e-administration, all of them based on adequate technical and organisational infrastructures. Relevant research issues can be to study the specific character of each dimension, how they relate to each other, the significance of and requirements to the infrastructures etc, taking into account the specific national social, political and cultural context. Rather than just looking for similarities, on should also identify differences and peculiarities.

References

Accenture (2001) "e-Government Leadership - Rhetoric vs. Reality: Closing the Gap", [online], http://www.accenture.com/xdoc/en/industries/government/final.pdf

Accenture (2002) "e-Government Leadership - Realizing the Vision", [online], http://www.accenture.com/xdoc/en/industries/government/egov_april2002_3.pdf

Accenture (2003) "e-Government Leadership: Engaging the Customer", [online], http://www.accenture.com/xdoc/en/industries/government/gove_capa_egov_leadership.pdf

Accenture (2004) "e-Government Leadership: High Performance, Maximum", [online], http://www.accenture.com/xdoc/en/industries/government/gove_egov_value.pdf

Adegboyega, Ojo, T. Janowski and E. Estevez (2005) Determining Progress Towards e_government: What are the core indicators? In Remenyi (Eds) Proceedings from 5thConference of e-Government University of Antwerp, Belgium 16-17 June 2005

Bakry, S. (2003) "Toward the development of a standard e-readiness assessment policy", International *Journal of Network Management,* Vol 13, pp129-137

Berg, H., Refsdal, F.O. og Holmen, L. (2005) *Datatilsynets bruk av IKT – en analyse av mål og rammeverk for e-forvaltning.* Avdeling for forvaltningsinformatikk, UiO. Juni 2005.

Bertelsmann Foundation (2001) "*Balanced e-government – Connecting efficient administration and responsive democracy".*

Bridge.org (2001) "*Comparison of e-Readiness Assessment Models"*, [online], http://www.bridges.org/ereadiness/report.html

Britannica online (2005): http://www.britannica.com/

Carbo, Toni, and Williams, J. (2004) "Models and Metrics for Evaluating Local Electronic Government Systems and Services", *Electronic Journal of e-Government*, Vol 2, Issue 2, pp 95-104

Capgemini (2005) *Online Availability of public services: How is Europe Progressing?* European Commission DG Information Society, Bruxelles.

COM (2003) *The Role of eGovernment for Europe's Future.* Communication from the Commission to the Council, COM (2003) 567 Final. Brussels 26.9.2003

Deloitte Research Public Sector Institute (2004) *At the dawn of e-government. The citizens as customer. http://www.deloitte.com/dtt/article/0,1002,sid%253D37085%2526cid%253D60672,00.html*

ECEG (2005) *Proceedings from 5thConference of e-Government* University of Antwerp, Belgium 16-17 June 2005. ISBN 1-905305-01-X

eEurope 2005: eEurope 2005 Action Plan Commission of EU. COM (2002) 263 final.

http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf

Eikeland, C. and S. Kongsrud (2005) *Utvikling av E-valuer – et rammeverk for å måle hvor langt kommuner er kommet i e-forvaltning*. Høgskolen i Agder, 2005.

EU (2001) Council of European Municipalities and Regions on eGovernance 28 November 2001.

FR (2004) *Forbrukerrådet*. http://www.forbrukerradet.no/

Grant, Gerald and Chau, Derek (2005): Developing a Generic Framework for E-Government. Journal of Global Information Management, 13(1), 1-30, Jan-March 2005
http://www.igi-online.com/downloads/pdf/ITJ2725_dGLKgMR9SK.pdf

Grannfland-Essers, I., and Ettedgui E. (2003) "Benchmarking e-Government in Europe and the US", Rand Europe

Grønlund, Å. Eds. (2002*) Electronic Government: Design Visions and Management*. Idea Group Publishing. 2002

Hacker, Kenneth L & van Dijk, Jan (2000): *Digital Democracy, Issues on Theory & Practice,* London: SAGE Publications.

Haug, Are Vegard(2003): *Politisk kommunikasjon på kommunale hjemmesider*, Oslo, Unipub Forlag. Også tilgjengelig på -

Haug, A.V. and Jansen, A. (2004) Municipalities enter the Internet – changed political communication? *Proceeding from European Conference on e-government,* Dublin 17-18. June 2004

Heeks, R. (1999) *Reinventing government in the information age*. London and New York Routledge. P 9-12.

Jansen, A. and S. Ølnes, (2004) Quality Assessment and Benchmarking of Norwegian Public Web Sites. *Proceeding from European Conference on e-government* 16-18.juni 2004 Dublin

Karim, Rais Abdul (1999) *Reengineering the public service:Leadership and change in an electronic age*. Subang Jaya Malaysia Pelanduk Publ.

Koh, C.E. and Prybutok, V.R. (2003) The three ring model and development of an instrument for measuring dimensions of e-government functions. *Journal of Computer Information Systems* 43 (3) 34-39.

Laye, K. and Lee. J. (2001) Developing fully functional e-government: A four stage model. Government Information Quarterly, 18 122-136.

Kvalitet 2005 (2005)*Kvalitetsmerking av offentlige nettsteder* http://www.norge.no/kvalitet/default.asp

OECD (2003) The case of e-government: Experts from the OECD Report "The E-government imperative." OECD Journal on Budgeting 3(1) 62-96

Osborne, D. and Gaebler, T. (1992) Reinventing government: How to entrepreneurial spirits is transforming the public sector. New York: Plume

Snijkers, K (2005) Balanced e-Government Implementations. In Remenyi (Eds) Proceedings from 5thConference of e-Government University of Antwerp, Belgium 16-17 June 2005

UN (2002) Benchmarking E-government: A Global Perspective - Assessing the UN Member States (2002) http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN021547.pdf

UN (2204) UN Global E-government Survey 2004 http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN019207.pdf

UN (2003) UN Global E-government Survey 2003. http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN016066.pdf

US government (2002) The e-government act of 2002. HR 2458. http://csrc.nist.gov/policies/HR2458-final.pdf

Ølnes, Svein (2001): Norwegian: Oppsummering av kvalitetsevaluering 2001, IN (English: Su*mmary of quality assessment*). Vestlandsforsking, VF-notat 7/2001. Sogndal

Ølnes, Svein (2003): Norwegian*: Kvalitesevaluering av offentlege vevtenester*, (English: *Quality assessment of public web-sites*) Vestlandsforsking, VF-rapport 9/2003. Sogndal.

4 PRIVACY IN RELATION TO NETWORKED ORGANISATIONS AND IDENTITY MANAGEMENT

Thomas Olsen, Tobias Mahler (NRCCL);
Clive Seddon, Vicky Cooper, Sarah Williams (Pinsent Masons);
Miguel Valdes, Sergio Morales Arias (Garrigues)

Abstract

This paper summarizes the findings of the study on privacy in relation to networked organisations and identity management, carried out by the Legal-IST project.[1] The focus of the study is on privacy and data protection aspects of networked organisations and on the use of identity management technologies, in particular multi-organisation single sign-on and federated identity management. In principle, both networked organisations and organisational networks to facilitate identity management may involve the processing of personal data, particularly if the networks are set up to serve consumers. From a data protection perspective, the main issue to be addressed is how the responsibility for processing personal data can be shared among the participants and the degree to which a network participant is legally responsible for collective processing of personal data. The study provides an analysis of the networking parties' duties and roles under data protection law and provides guidelines and model contracts to comply with the legal framework. The European data protection framework for collaborative networks is highlighted, including selected recommendations of the Art 29 Working Party of the European Directive on Data Protection. Organisational networks to facilitate identity management are discussed both in relation to government-built networks and,

1 Legal-IST (Legal issues for the Advancement of Information Society Technologies) is an EU funded research project under the 6th framework programme. The objectives of Legal-IST include amongst others to support the research activities within the IST priority from a legal point of view, by studying the legal implications of current research initiatives in IST (in terms of both new emerging technologies and relevant networked business models) and to provide suggestions for relevant implementation strategies. The full report on Privacy in Relation to Networked Organisations and Identity Management is expected to be available early 2006 on the project's website (www.legal-ist.org).

in particular, in relation to identity management schemes set up by a network of enterprises.

1. Introduction

The study covers three aspects, which are of core importance to the Information Society Technologies domain, namely the protection of privacy, the uptake of new technologies and the new business models that are facilitated through these technologies.

Privacy is a fundamental right, recognised not only on the European level. Privacy is also recognised – on the basis of various international surveys- as a precondition for enhancing trust and thus growth of e-commerce activities. Privacy is also recognised by EU Ministers as a precondition for e-government services. On the one hand, privacy is becoming a part of the European social and legal culture, but on the other, new electronic products, services and methods may affect privacy. Privacy concerns may even inhibit the uptake of certain technologies, as the failure of Microsoft's intended general use of the .Net Passport Identity Management system shows. Identity Management can be understood[2] as an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users' access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems. Single sign-on and federated identity management represent the most business-driven solutions for letting customers have access to multiple web sites and resources after a single authentication procedure. Federated identity management consists both of a technology that facilitates the communication of identification data and of a network of collaborating organisations, which allows the creation of new collaborative business models.

Identity Management Systems (IMS) and particularly privacy-enhancing IMS present an important research focus for many European research projects and for international collaborations. The technologies that currently are under development and the way these will be implemented will probably have a major impact on the way we will communicate and collaborate through the Internet in the future. It is therefore important that researchers and those implementing the technologies are aware of the legal framework.

2 See e.g. http://en.wikipedia.org/wiki/Identity_management.

Due to the focus on privacy and data protection, the study does not address other relevant legal issues that may arise in relation to IMS systems. For example, there may be liability issues, which fall outside the scope of this report. Moreover, the legal framework for digital signatures and PKI (Public Key Infrastructure) is relevant, but can not be addressed here. Particular legal issues may also arise from the use of technologies such as RFID and biometrics.

2. Relation to other IST projects and benefits for the stakeholders

The study's focus on organisational collaboration is complementary to other research projects in the IST domain, particularly the integrated projects PRIME and GUIDE. GUIDE is conducting research and technological development with the aim of creating architecture for secure and interoperable e-government electronic identity services and transactions for Europe. PRIME is focusing on the design and development of practical, federated IMS that effectively and reliably enforce privacy. Compared to these projects, the Legal-IST study focuses more on identity management in the context of collaborating controllers and on compliance with data protection law using readily available IMS. This double focus on data protection aspects of organisational collaboration as well as on data protection aspects of identity management technologies is the essentially new contribution made by this Legal-IST study.

The aim of the study is to assist networked organisations and identity management networks:

- by facilitating an understanding of general privacy and data protection issues;
- by highlighting how the responsibility for compliance with data protection law can be administrated in a network;
- by analysing the data protection issues in relation to example IMS solutions; and
- by providing example contract clauses that can be taken as a point of departure for more specific clauses in a particular network.

3. Data Protection Law

Data protection laws include a number of requirements for collaboration between members of a network of organisations and businesses. The study reviews the general duties under European data protection law and highlights how these duties apply to networked organisations. The general duties includes among others roles and responsibilities, criteria for lawful processing, infor-

mation to be provided, data quality, data subjects rights, notification and entry in the register, security and international movement of personal data. A major part of the study is a detailed analysis of data protection issues in to the context of collaborating data controllers. Another major part of the study is on the specific legal issues of collaboration through the means of IMS.

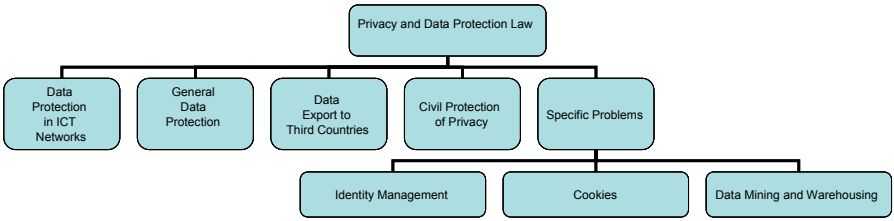


Figure 1. Privacy and data protection – structure amended from Legal-IST D01, figure 14.

The study addresses a number of sub-areas identified in the Legal-IST report "Legal research state-of-the-art", (D01), in particular issues related to data protection in ICT networks and international data flow including data export to third countries. Identity management can be envisaged as a specific problem related to these areas.

The point of departure in the study has been to analyse such data controllers' duties under EU data protection law. Since the Data Protection Directive (95/46/EC) and the E-communications Directive (2002/58/EC) provide for harmonisation of the data protection laws in the EU and European Economic Area (EEA)[3], our analysis of these instruments reflects the legal situation in the EU/EEA Member States. National laws in the UK, Spain and Norway have been analysed on specific issues where the Directives do not provide much guidance or are unclear, e.g. on the legal aspects of jointly controlling the processing of personal data. The analysis of these national laws shows that there are some divergences with regard to how the directives have been implemented. Controllers should therefore always consider the relevant national law and practice, and if necessary seek legal advice regarding their specific needs.

3 The EEA consists of the EU Member States including the EFTA Member States Norway, Island and Liechtenstein.

4. Networked Organisations and Data Protection Law

The term "networked organisation" is not a firmly established concept. The term is used in parts of the literature to cover a variety of collaborations between different organisations.[4] The term is meant to cover different forms of collaboration between organisations, including, Virtual Communities of Companies, Virtual Organisations, Virtual Enterprises and Professional Virtual Communities.

From an organisational perspective there are different degrees of collaboration between organisations. A very limited collaboration may consist in the mere occasional exchange of information; a more advanced collaboration may involve the sharing of some responsibilities in selected aspects; a full collaboration would entail the sharing of all responsibilities. As soon as such collaborations involve the processing of personal data, collaborators must be aware of their responsibilities in relation to their use of personal data.

Different degrees of collaboration need to be reflected in the roles that are available under European data protection law. Some collaborators in a networked organisation may be restricted to the processing of personal data on behalf of others (data processors). Other collaborators may qualify as responsible data controllers. Networked organisations processing personal data can therefore also be understood as networks of data controllers and data processors. Our main focus is directed at the data controllers, since they determine the purposes and means of the data processing and bear the main responsibility for compliance with data protection law.

According to Article 2(d) of the EC Data Protection Directive, the processing of personal data can be carried out either alone or jointly. This allows for different forms of collaboration, which are illustrated in figure 2.

4 L Camarinha-Matos and H Afsarmanesh Collaborative networked organizations: a research agenda for emerging business models (Springer New York 2004), p. 10.

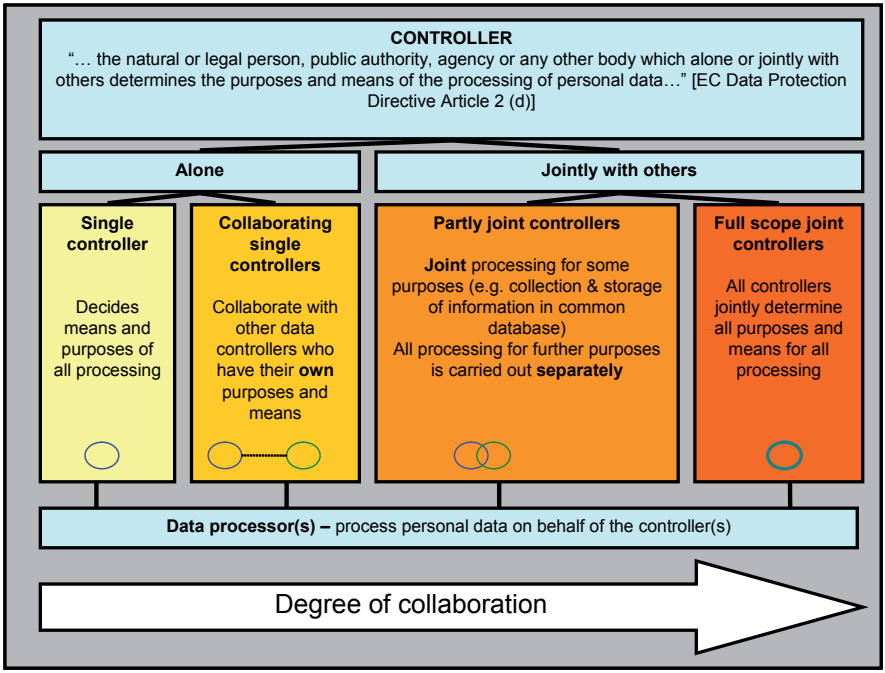


Figure 2. Collaboration between data controllers.

5. Recommendations for networked organisations

- Data protection issues should be addressed at an early stage of network development if the networked organisation will handle personal data.
- The business processes of the networked organisation should be analysed in order to identify data protection roles (data controller and data processor). Consider in particular if there will be instances of joint processing or if all processing will be carried out by separate controllers. Data controllers should consider if they in fact are jointly determining the means and purposes of the processing. Parties should also be aware of the possibility that the network operations involve more than one processing, and that the different instances of processing may have different controllers.
- If the business process analysis indicates that there may be instances of joint processing, be aware that there may be considerable differences in national laws with respect to how data protection authorities regard joint processing. In many countries the principle of purpose limitation (perso-

nal data shall only be used for legitimate and specified purposes and shall not be further processed for purposes incompatible with the purposes for which the data are first collected) will be considered as a major limiting factor for the possibility to choose a collaboration structure involving joint processing.

- Joint controllers should define clear roles and responsibilities with regard to the processing of personal data. It is of particular importance to ensure that data subjects are provided with relevant information about the processing and that the joint controllers in practice are able to fulfil their responsibilities like e.g. to facilitate the execution of the data subject's right to access his or her personal data. Networked organisations should consider whether one of the joint processors should be responsible for fulfilling these more practical tasks.
- For all relations between data controllers and data processors the law requires a contract that makes the responsibilities explicit. We recommend that collaborating data controllers also set up such contracts. Templates are provided in the appendices of the report.

6. Identity Management and Data Protection Law

The focus of identity management is on how to rationalise pre-registration, authentication and authorisation procedures. Before the creation of the Internet, most organisations carried out identity management themselves. However, with the Internet came also the opportunity to have some of these processes performed by third parties. Many companies have seen the opportunity to rationalise by having common procedures and infrastructures. Even more important, however, is the opportunity companies have seen in providing customers easy access across company web sites. Single sign-on and federated identity management represent the most business-driven solutions for letting customers have access to multiple web sites and resources after a single authentication procedure.

Key benefits associated with federated identity management are:[5]

- Convenience to users as they can more seamlessly move between services using a single username/password pair;
- Cost savings for organisations arising from a shared scheme based on standardised, interoperable architecture;

5 See R Clarke Identity Management – The technologies, their business, their problems, their prospects (2004) pp. 12-17. See also Liberty Alliance Business Benefits of Federated Identity (2003) and Benefits of Federated Identity to Government (2004).

- Possibilities for organisations to focus on their distinctive competencies by outsourcing authentication and identity management to professional Identity Providers;
- The possibilities of new business models,
  - organisations that already have significant customer bases can pass them on to other sites an gain referral and commission fees;
  - organisations and service providers may more easily get in contact customers interested in their services;
- Support for sites to customise and personalise their services based on profiles associated with user accounts;
- Governments may simplify the access to services and applications both government to government, government to citizens, but also government to business.

The study introduces basic concepts, functions and models for identity management. The current status of identity management is shown both through an evaluation of available IMS and via perspectives taken by ongoing R&D projects focusing on privacy-enhancing identity management. The study discusses the two most prominent examples of identity management systems, Microsoft .Net Passport and the Liberty Alliance Project with regard to compliance with data protection law. The study also provides contractual templates that can be taken as a point of departure for more specific clauses in a particular network using IMS.

As emphasized e.g. by the Article 29 Working Group, it is important for the parties involved in an identity management network to set up clear contractual agreements that reflect roles and responsibilities. The report aims to assist collaborators:

- by facilitating an understanding of general data protection issues;
- by highlighting how the responsibility for compliance with data protection law can be administrated in a network;
- by analysing the data protection issues in relation to example IMS solutions; and
- by providing example contract clauses that can be taken as a point of departure for more specific clauses in a particular network.

7. Recommendation for organisations setting up an Identity Management System (IMS)

- To a certain degree the design of an IMS will involve the establishment of a network of organisations. Hence, the above recommendations regarding networked organisations should equally be considered when setting up an IMS.
- Data protection issues should be addressed at an early stage of network development since the Identity Management System in most cases will handle personal data.
- The parties setting up an IMS are themselves responsible for compliance with data protection law. The use of standards and specifications like those provided by Liberty Alliance do not necessarily ensure compliance with data protection law.
- Those defining specifications for Identity Management are usually not responsible controllers or processors under data protection law. Hence, they are in most cases not legally responsible for compliance, but they should nevertheless ensure that the specifications facilitate the development of compliant systems.
- Organisations setting up an IMS should be aware of the roles they will play in the network. In particular they should consider if they will act as data controllers, data processors or both. Particular attention should also be given to the roles defined in the E-communications Directive, i.e. public electronic communications network and services providers.
- The end users of the Identity Management System should be provided with relevant information about its functioning and the responsibilities of the participating organisations.

8. Recommendations for the EU Commission

Recommendations regarding networked organisations

- The EC Data Protection Directive (95/46/EC) and the E-Communications Directive (2002/58/EC) provide a general framework that is adequate for networked organisations. Both directives define roles that are relevant for organisations participating in a network where personal data is handled. In practice, a networked organisation will consist of collaborations between separate controllers, joint controllers, and all of these may outsource some work to processors. Amongst these forms of cooperation, the concept of joint data controllers appears as the most problematic. The

Data Protection Directive does not clearly define rules for joint processing, and there seem to be considerable differences in national laws and with respect to how data protection authorities regard joint processing. Hence, the role of joint processing under European data protection law should be reconsidered. While the concept of joint processing should not necessarily be abolished, we consider that there is a need for clarification.
- Future research should focus on experiences with and consequences of joint processing. Such research could e.g. examine whether and how organisations manage to set up a suitable framework for joint processing and how the division of responsibilities affects data subjects and is perceived by them.

Recommendations regarding IMS

- IMS may prove to be important cornerstones in the architecture of communication between individuals and multiple service providers. Both design and actual implementation have a high potential impact on privacy consequences of such systems. If data protection issues are ignored, this may have significant consequences for the involved users, since such systems may facilitate the accumulation of detailed profiles of their use of digital identities. This may in turn have a negative impact on the uptake and acceptance of the IMS, as illustrated by the Microsoft .Net Passport case. Some of the challenges in IMS may be solved by giving research on privacy enhancing identity management a continued high priority.
- The European legal framework for data protection law provides mainly adequate rules for setting up an identity management system that ensures fair processing of personal data. However, the rather general rules are difficult to apply, it is e.g. difficult to map the roles defined in data protection law with the roles included in a typical IMS, involving e.g. identity providers, attribute providers and service providers.
- European data protection law applies to the processing of personal data, while the handling of anonymous data in principle falls outside its scope. A third concept, which is of a particular importance in relation to IMS, is pseudonymity. This concept has a rather unclear position in European data protection law, and only a few, mostly national, rules refer to the concept. It is in practice difficult to determine whether pseudonyms should be considered as personal data. The examples from the studied identity management frameworks illustrate that the concept of pseudonymous data spans from a globally unique identifier, which is broadly available in a multi-organisation IMS, to an opaque handle (as defined by Liberty Alliance), which is available only to a limited set of service pro-

viders (normally two) and which can only be understood by those. One of the most important safeguards against extensive and privacy-intrusive profiling is to prevent the possibility of merging local profiles from different domains. The use of pseudonyms is useful to ensure that users are not identifiable by third parties, while they still may be identified and held responsible by a trusted party when identification is justified. From a privacy perspective it would be advantageous to

- further encourage the development and use of anonymous and pseudonymous services,
- clarify the normative status of pseudonymity, and to
- provide clearer rules about the use of pseudonyms.

- The further development of IMS should be closely followed by the Art. 29 Working Party. A general challenge for national and international supervisory authorities is that they have a competence to review only the implementations of information systems. At this point of time, the underlying specifications that define the functioning of the system are already set and may be difficult to amend. This emphasizes the need of considering data protection issues at an early stage of development.

5 LEGAL RISK ANALYSIS WITH RESPECT TO IPR IN A COLLABORATIVE ENGINEERING VIRTUAL ORGANIZATION[1]

Tobias Mahler (NRCCL) and Fredrik Vraalsen (SINTEF)

Establishing and operating a virtual organization implies a number of challenges from many different perspectives, including socio-economic, organizational, legal and computational issues. This paper focuses on the legal aspects with a particular view on legal risks with respect to intellectual property rights. A risk analysis with respect to legal issues can either be based on abstract legal reasoning or it can focus on the business reality and the specific characterizations of the virtual organization. This paper follows the latter approach; it presents selected findings of a legal risk analysis of a business scenario in the collaborative engineering field. The legal risk analysis was performed in collaboration between lawyers and other professionals in order to highlight how different legal and non-legal aspects relate to each other. Graphical models of risks and treatments were utilized in order to reduce communicational barriers between experts in this multidisciplinary setting.

1. Introduction

A virtual organization (VO) can be understood as a temporary or permanent coalition of geographically dispersed individuals, groups, organizational units or entire organizations that pool resources, capabilities and information to achieve common objectives (Dimitrakos et al 2004).

From a legal point of view, it is advisable to base the establishment and operation of a VO on a clear contractual basis, which outlines rights and duties of the VO participants. An example of such a contract is outlined e.g. in (ALIVE 2002a). The ALIVE template provides a good starting point for negotiating contracts for VOs where the partners will collaborate on a medium-term to long-term basis, similar to a joint venture.

---

1 This is an updated version of a paper published in Collaborative Networks and their Breeding Environments, proceedings of the Sixth IFIP Working Conference on VIRTUAL ENTERPRISES, Valencia 26.09.2005 - 28.09.2005, New York 2005.

There is no general European legal framework for the establishment and operation of virtual organizations, thus legal issues in relation to VOs are still a topic for research. A recently published *strategic roadmap for advanced virtual organizations* points out that the analysis of legal risks arising in operating VOs and the development of legal strategies to overcome them is an important research task in order to support collaborate networked organizations (Camarinha-Matos et al. 2004, p. 296). One area where VO participants face a number of legal risks is the protection of intellectual property rights (IPR), which is the focus of this paper.

Others have addressed risk management for projects (e.g. Baccarini & Archer 1999, Raz & Michael 1999), focusing on general risks for the project as such. Compared to these approaches, this paper focuses not on general risks but only on risks that can be related to legal issues; in this sense it is more specific. The legal risk analysis presented in this paper utilized some of the UML-based graphical models for risk analysis developed by the CORAS IST project to facilitate documentation and communication of risk analysis results (den Braber et. al. 2005). The goal of the analysis was twofold; 1) to identify legal risks and treatments related to IPR in the selected VO scenario, with the aim to create a set of reusable results for use in future analyses, e.g. in the form of templates and checklists, and 2) to evaluate the suitability of risk analysis, in particular the CORAS model-based risk analysis (MBRA) methods and graphical language, with respect to supporting the analysis of legal issues in relation to contract formation in VOs.

The remainder of this paper is structured as follows: Section 2 describes how legal risk analysis can be performed utilizing graphical models; section 3 introduces the collaborative engineering scenario which is the basis for the analysis; section 4 outlines the role of IPR issues in VO-related contracts; section 5 presents selected results of the legal risk analysis performed on the basis of the scenario. Finally, section 6 draws the main conclusions.

2. Legal risk analysis

The establishment of a VO often occurs under the pressure of time in order to avoid losing the business opportunity which is the primary driver for the collaboration. On the other hand, the parties need to define a contract that sets out the internal functioning of the VO; the contract is a key mechanism for the VO management.

In such cases it is advisory to base the contract on an existing template. However, such contractual templates can not be used “off the shelf”; they need to be adapted to the needs of the specific VO. This implies an adjustment of the contractual rules, taking into account the specific aim of the collabora-

tion, how the partners want to organize the internal management of the VO, whether the VO structure is more static or more dynamic, and what kinds of specific risks have to be taken into account.

Legal risk analysis (LRA) can be applied to the process of adjusting a contract template to the specific risks of the VO. The VO needs to avoid two situations: First, the contract should not overlook relevant risks that should have been addressed in the contract. Second, the contract should avoid addressing issues that are of little business relevance and where the related contractual terms would themselves present a barrier for a successful collaboration, e.g. by providing very bureaucratic rules for cooperation.

For the purpose of this paper, we define LRA as a risk analysis that focuses on the one hand on risks that stem from the legal domain (e.g. loss of a legal right) and on the other hand on non-legal risks that can be treated with legal means. The advantage of this rather broad understanding is that it provides an integrated approach, where legal risks also can be treated by non-legal means and non-legal risks may be addressed with typically legal approaches, e.g. a contractual rule.

2.1 Model-based Risk Analysis

Risk analysis requires a clear understanding of the system to be analysed. Normally, this understanding can be obtained only through the involvement of different stakeholders, e.g. legal experts, security experts, system developers and users. In fact, most methods for risk identification make use of structured brainstorming sessions of one kind or another, e.g. Hazard and Operability (HazOp) analysis (Redmill et. al. 1999), involving 5-7 stakeholders and domain experts with different backgrounds. The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. The CORAS language for threat modelling (den Braber et. al. 2005) has been designed to mitigate this problem within the security domain. Recent work has focused on application of the CORAS language and methodology to the analysis of legal issues (Vraalsen et. al. 2005).

The CORAS language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand icons (symbols) associated with the modelling elements of the language. The CORAS language is an extension of the UML 2.0 (OMG 2004a) specification language, the de facto standard modelling language for information systems. It is defined as a UML profile (Lund et. al. 2003), and has recently become part of an OMG standard (OMG 2004b).

3. Collaborative engineering scenario

This section presents the scenario which is being used in the remainder of the paper. It is a simplified version of a collaborative engineering scenario from the aerospace industry which is being used in the TrustCoM IST project (www.eu-trustcom.com) as part of a test bed. It is being analyzed from different perspectives, including computational aspects, socio-economic aspects and legal aspects. A similar version of this scenario is described by Wesner et al. (Wesner et al., 2004), who focus more on computational aspects.

The scenario addresses a collaborative engineering project typical of the aerospace industry, where a lead contractor collaborates with a large number of subcontractors and peer organizations on the development of an airplane or similar product over a 15 year time period, followed by a 20-40 year deployment period. The TrustCoM collaborative engineering scenario consists of three VOs:

- An airliner VO, (Air VO) consisting of the carrier, support and maintenance teams;
- A Collaborative Engineering VO, (CE VO) which has the technical expertise to specify, design and integrate systems into complex products, and which may also manufacture the solution for the customer. This VO's business goal is to win a contract with the Air VO regarding the upgrade of a particular aircraft type with a new feature. One of the partners of the CE VO, the Systems Integrator (SI), is specialized in the integration of different aircraft systems.
- A number of engineering analysis consultancies that form a VO to support design activities within engineering companies. The Analysis VO (AVO) supports general analysis work across engineering and scientific sectors.

The themes covered by TrustCoM in this scenario include:

- Design and analysis data security; protection of intellectual property;
- Enforcement of Trust and Security policies through the interpretation of contracts and by reacting to notable business 'events';
- Contract negotiation between clients and service providers to support collaborative agreements and service level agreements.

Whilst the main focus of this paper is the protection of IPR in a contractual context, we also attempt to relate the legal issues to the trust and security issues addressed by other parts of the TrustCoM project.

4. Intellectual property rights in vo contracts

A number of different contracts will govern the internal and external relations in the scenario. These will include at least the following types of contracts: (1) VO-internal consortium agreements, which establish consortia of organizations with respective VO goals. All CE VO members will be parties to a consortium agreement. (2) Contracts about the provision of a service or the purchase of a good, without establishing a consortium. This type of contract will be in place between the CE VO (possibly represented by a lead contractor) and the two other VOs, AVO and Air VO. Both types of contracts should also cover IPR issues.

Intellectual and industrial property (IP) rights consist of a variety of rights, including copyright, database protection, patent protection, trademark and design protection and the protection of confidential information (i.e. know-how and trade secrets). The legal framework for these rights shows some variations, taking into account the nature of the protected intellectual property. The law is regulated in slightly different ways in the various member states of the European Union, despite a harmonization of selected IPR issues in European law.

For a VO, the protection of copyrights is closely related to the question of legal personality. In principle, only an entity with legal personality can hold legal rights. Therefore, if the VO has legal personality, it can hold most intellectual property rights. VOs that lack legal personality must refer to their members as holders of all legal rights. A general analysis of IPR issues in a VO context was carried out by the ALIVE project (ALIVE 2002b).

Relevant IPR issues that are likely to be encountered in the formation and operation of a VO can, for the sake of simplicity, be split into two principal categories: Internal issues arise among the various members of a VO, whereas external issues arise between the VO and/or its members, on the one hand, and parties outside the VO on the other hand. We should also make a distinction between pre-existing IP, which is brought into the VO by the partners, and the IP developed during the co-operative process.

5. Selected results of the legal risk analysis

This section presents selected results of the legal risk analysis, which was performed according to the CORAS risk analysis process. The initial step of this process consists of describing the context of the analysis, i.e. the target of analysis and relevant stakeholders and assets. The target for the risk analysis was the scenario presented in section 3, with a focus on the analysis of IPR, as detailed in section 4, in particular know-how and trade secrets (confidential

information). The analysis was performed from the viewpoint of the airplane Systems Integrator (SI) partner of the CE VO.

The risk identification was performed during a number of HazOp brainstorming sessions involving participants with backgrounds in law, engineering, economics, computer science and philosophy. Risks were assigned consequence and frequency values and prioritised, and treatments were then identified for the major risks through another brainstorming session. Some examples of identified risks and treatments are presented below.

5.1 Example of Identified Risks

The identified risks relate to different IPR issues, including the protection of confidential information (i.e. know-how and trade secrets), the ownership of IP and liability for IPR infringements by other VO partners. It would be outside the scope of this paper to present all identified risks. We will therefore concentrate on risks related to the loss of confidential information, which was identified as a major risk category. The internal collaboration in the CE VO and its cooperation with the AVO and the Air VO, respectively, may imply that confidential information is shared or otherwise disclosed to VO partners or to external parties. This involves a risk that such confidential information is disclosed to third parties or used by VO members for purposes that are not related to the VO.

Figure 1 shows a CORAS UML diagram describing some ways in which confidential information can be disclosed and potential consequences this disclosure may have. In the CORAS language for risk analysis a threat is described using a *threat agent*, e.g. a disloyal employee or a computer virus, typically represented in the diagram by a stick figure. The threat agent initiates a *threat scenario*, which is a sequence of events or activities leading to an *unwanted incident*, i.e. an event resulting in a reduction in the value of the target *asset*. Furthermore, an unwanted incident may initiate or lead to other unwanted incidents, forming chains of events. For example, an unfaithful employee working for one of the CE VO partners may have access to confidential information which he/she could disclose to a third party. This disclosure could lead to the information reaching the public domain and thereby losing its legal protection and value as a trade secret. A similar but opposite scenario is that an employee of our stakeholder (SI) is unfaithful and discloses the client's confidential information. This again could lead to the CE VO or the SI being sued for breach of the non-disclosure agreement with the Air VO. The latter unwanted incident may not only have consequences for the SI's revenue, it may also lead to further consequences, like negative publicity.

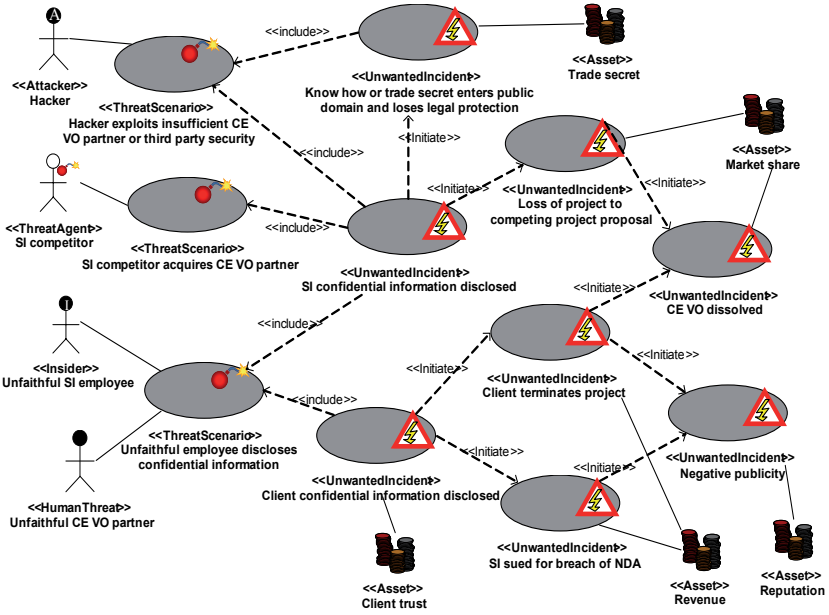


Figure 1 Confidential information loses legal protection

5.2 Example of Identified Treatments

For each of the risks, we have explored potential treatments related to three main areas of the TrustCoM project, namely trust, security and contracts. Our aim was to develop an integrated set of treatments, where legal and other measures are integrated. In this context we focused on law as a proactive mechanism, which tries to solve legal issues before they arise; legal reactions *ex post* were not addressed.

Treatments may have different effects on risks, they may e.g. reduce the consequence or frequency of the unwanted incident occurring, or transfer the risk to another party, e.g. through insurance. A selection of treatments to the risks described above is shown in the CORAS treatment diagram in Figure 2. Two of these treatments are clearly within the legal domain: First, a contract clause could avoid the disclosure of confidential information in case of a merger or acquisition, by allowing a re-negotiation of the general VO agreement in this event. Second, specific contractual rules in the VO agreement should address the VO members' liability towards third parties. The remaining treatments involve

legal and non-legal elements: Information security mechanisms like limitations to storage time and the deletion of data after an analysis are of key importance. Such mechanisms can be made obligatory via contractual clauses in the agreement between the CE VO and the AVO. If the technology was available, a VO-internal enterprise Digital Rights Management (DRM) system could also reduce the likelihood of confidential information being disclosed, particularly if some of the contractual obligations could be enforced through technology.

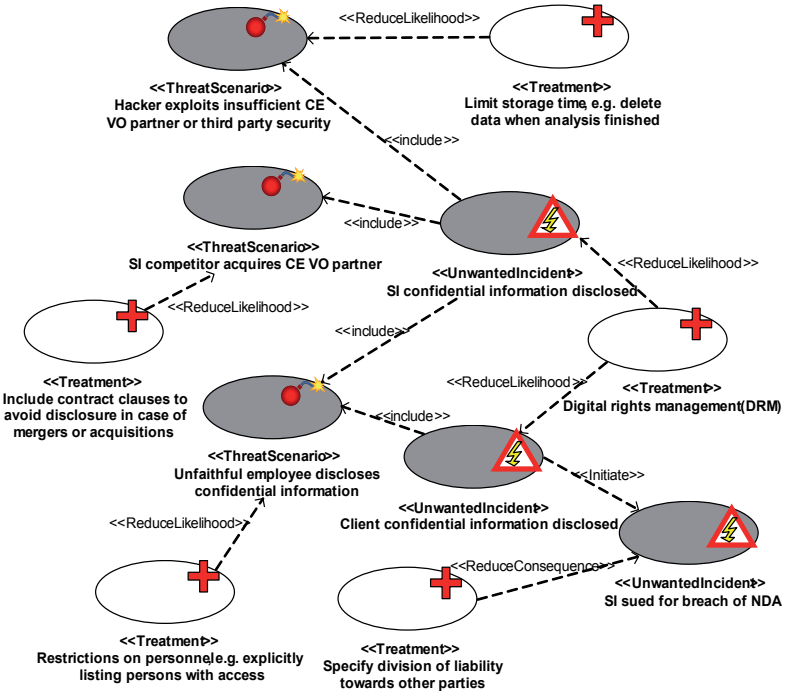


Figure 2 Risk treatments

6. Concluding remarks

We have presented results from the analysis of a collaborative engineering VO scenario, where a number of legal risks and treatments were identified. Our risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management.

Interestingly, many of the relevant contractual treatments were also included in a general manner in the ALIVE contract template for VOs (ALIVE 2002a). The performed legal risk analysis provided indications about how these rules can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template.

The analysis results were generated during a number of brainstorming sessions involving participants with varied backgrounds, including law, computer science, engineering, economics and philosophy. Based on our experiences, the graphical models can indeed facilitate the communication and understanding with respect to legal issues in a multidisciplinary context. Ongoing work is focusing on further adapting the CORAS methodology and graphical language to better suit legal risk analysis (Vraalsen et. al. 2005), as well as on creating reusable elements in the form of e.g. checklists based on the results of this analysis in order to facilitate future analyses.

7. Acknowlegements

The results presented here are partly financed by the European Commission under contract IST-2003-01945 through the project TrustCoM and partly financed under the Research Council of Norway through the project ENFORCE.

We would like to acknowledge the work done by David Goldby from BAE Systems, who has defined the collaborative engineering scenario for TrustCoM. We would also like to thank David Goldby, Mass Soldal Lund, Xavier Parent and Claudia Keser for participating in the risk analysis sessions.

8. REFERENCES

ALIVE IST Project (2002a). Report D 17 a, VE Model Contracts, available at http://www.vive-ig.net/projects/alive/docs.html.

ALIVE IST Project (2002b) *Report D 13, ALIVE Project, Intellectual & Industrial Property Rights Legal Issue Subgroup*. http://www.vive-ig.net/projects/alive/docs.html.

Baccarini, D. and Archer, R. *The risk ranking of projects: a methodology.* International Journal of Project Management 19 (2001) 139-145.

Folker den Braber, Mass Soldal Lund, Ketil Stølen, Fredrik Vraalsen. The CORAS methodology: Model based security analysis using UML and UP. Encyclopedia of Information Science and Technology. Information Resources Management Association, USA (2005)

Camarinha-Matos, L., Afsarmanesh, H., Löh, H., Sturm, F., Ollus, M. A strategic roadmap for advanced virtual organizations. In collaborative networked oganizations: a research agenda for emerging business models. Camarinha-Matos, L and Afsarmanesh, ed. New York: Springer 2004.

Dimitrakos T, Goldby D and Kearney P. Towards a trust and contract management framework for dynamic virtual organizations. In E-Adoption and the knowledge economy: eChallenges 2004, IOS press 2004.

Lund, M.S., Hogganvik, I., Seehusen, F., Stølen, K.: UML profile for security assessment. Technical Report STF40 A03066, SINTEF Telecom and informatics (2003).

OMG: UML 2.0 Superstructure Specification. (2004a) OMG Document: ptc/2004-10-02.

OMG: UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms, Draft Adopted Specification (2004b) OMG Document: ptc/2004-06-01.

Raz T and Michael E. Use and benefits of tools for project risk management. International Journal of Project Management 19 (1999) 9-17.

Redmill, F., Chudleigh, M., Catmur, J.: HazOp and software HazOp. Wiley (1999)

Vraalsen, F., Lund, M.S., Mahler, T., Parent, X. and Stølen, K. Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experiences and the Way Forward. In Proceedings of the 3rd International Conference on Trust Management (iTrust '05). Paris, France, May 2005. Springer LNCS 3477.

Wesner S, Schubert L, Dimitrakos T. *Dynamic Virtual Organizations in Engineering*. Forthcoming, the Proceedings of the Second German-Russian Workshop. Notes on Numerical Fluid Mechanics and Multidisciplinary Design (NNFM). Springer.

6 SIS II LEGISLATIVE PROPOSALS 2005: GAINS AND LOSSES!

Stephen K. Karanja

1. Three Proposals

On 31 May 2003 the Commission issued the long awaited Schengen Information System II (SIS II) proposal legislation. The legislative law consists of three proposals: two Regulations and a Decision. The first proposal Regulation is based on Title IV of the Treaty establishing the European Community (TEC),[1] and the Decision based on Title VI of the Treaty on the European Union (TEU)[2]. Both instruments lay down provisions on the architecture, financing, responsibilities and general data processing and data protection rules for the SIS II. Apart from these common rules, the Decision contains specific provisions regarding the processing of SIS II data for supporting police and judicial cooperation in criminal matters, while the Regulation rules on the processing of SIS II data supporting the implementation of policies linked to the movement of persons, part of the Schengen acquis, external borders and visa.[3]

The second Regulation is based on Title V TEC (Transport) regarding the specific issue of access to the SIS II by the authorities and services in the Member States responsible for issuing registration certificates for vehicle.[4] The purpose is to guarantee that the services responsible for issuing registration certificates for vehicles shall have access to the same SIS data under the new legal framework for SIS II as they will have when the 2003 proposed Regulation enters into force.[5]

---

1 Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), COM(2005) 236 final, 31.5.2005

2 Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II), COM(2005) 230 final, 31.5.2005.

3 COM(2005) 236 final, p. 4 and COM(2005) 230 final, p. 4

4 Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, COM(2005)237 final, 31.5.2005.

5 COM(2003) 510 final – 2003/0198; Text will be revised in case the Proposal from August 2003 is adopted.

All the legal instruments are to be adopted in due time for allowing the necessary preparations to the new system and, in particular, the migration from the current system to the SIS II. The effect of the proposals is to repeal and replace the current SIS law which is based on the Schengen Convention Articles 92 – 119 and the Decisions and Declarations of the Schengen Executive Committee which related to the SIS.[6] Further the first Regulation and the Decision will also repeal Regulation (EC) No 378/2004 of 19 February 2004 on procedures for amending the SIRENE Manual.[7]

This article examines the changes brought about by the legislative proposals and compares them to the current SIS rules to determine the gains and losses for the Schengen data processing and data protection rules.

2. SIS II and Legislative Proposals

2.1. Purpose and Policy Aims

In Article 2, both the Regulation and the Decision define the purpose and policy aims of the proposal legislation. The legislation defines conditions and procedures for the processing alerts and additional data relate to them in the SIS II and the exchange of supplementary information for purposes of police and judicial co-operation in criminal matters (the Decision) and for the purpose of refusing entry into the territory of the Member States (the Regulation). The legislation also lays down provisions on the technical architecture of the SIS II, responsibilities of the Member States and the Commission, general data processing, rights of individuals concerned and liability.

According to Article 1 of both the Regulation and the Decision the purpose and aims of SIS II are to enable competent authorities of Member States to co-operate by exchange of information for the purposes of controls on persons and objects and contribute to maintaining high level of security within an area without internal border controls between Member States.

The new legislation upholds the same purpose and policy aims as the Schengen Convention and current SIS law. However, the new law is more precise that the policy aims are to maintain high level security within Member States territories by exchanging information on persons and objects. Security is therefore given higher prominence than free movement.

---

6 COM(2005) 236 final, p. 4; also Article 36 and COM(2005) 230 final, p. ; also Article 62

7 OJ L 64, 2.3.2004, p. 5 & 45 respectively; See also Articles 63 of the Decision and 37 of the Regulation.

2.2. Legal Basis

The new legislation allocates the SIS its appropriate legal basis. Under the Amsterdam Treaty, the legal basis of Schengen acquis was divided between the first pillar and the third pillar. Council Decision 1999/436/EC of 20 May 1999[8] determined the legal basis in the Treaties for each of the provisions or decisions of the Schengen acquis but the Council did not reach a decision on the provisions regarding the SIS. Despite the SIS acquiring dual legal base with the transfer of matters concerning immigration and border crossing to the first pillar, the provisions of the SIS were regarded as acts based on Title VI TEU, the third pillar. The SIS II law therefore allocates the SIS its appropriate legal basis in the Treaties as required by Article 5(1) of the Schengen Protocol annexed to the Amsterdam Treaty. The two instruments, the Regulation and the Decision reflect the dual nature of the Schengen acquis. The Regulation has its legal basis in Title IV TEC which deals with visa, asylum, immigration and other policies related to the movement of persons. While the Decision has its legal basis in Title VI TEU concerned with police and judicial co-operation in criminal matters.

The legal basis of the second Regulation proposal is Article 71(1)(d9 TEC.[9] The choice for the legal basis signifies that access to the SIS by vehicle registration services has a basis in the EC Treaty.[10] The Regulation replaces Article 102a of the Schengen Convention.

Although the SIS II legislation makes clear the legal basis of different aspects of the SIS, it falls short of what many Schengen commentators have advocated for, namely the transfer of the entire Schengen acquis to the first pillar. The dual legal basis of the SIS means that there continues to be two levels of data protection one under the EU Directive 95/46[11] and EC Regulation 45/2001[12] and the other under the CoE Convention[13]. This is poor for data protection. A common level of data protection would have been preferable. But on a positive note, the incorporation of the SIRENE (Supplementary Information Request

8 OJ L 176, 10.7.1999, p. 17.
9 COM(2005)237 final 2005/01404 (COD) p.3
10 Ibid. p. 5
11 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
12 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 8 of 12.1.2000)
13 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS no. 108 of 1981

at the National Entries) in these instruments means that the SIRENE now has a proper and certain legal basis within the Treaties.

2.3. Organisational Overview

2.3.1. Technical Structure

The technical structure of SIS II will be different from that of the current SIS which consists of two parts: the central SIS and the National SIS. SIS II will consist of three parts (see Figure 1): First is a central database called 'the Central Schengen Information System (CS-SIS), which will contain all data entered by Member States. Second, one or two access points or national interfaces defined by each Member States (NI-SIS). The National Systems of Member States (NS) is to be connected to the SIS II via the NI-SIS. Each Member State has the responsibility for operating and maintaining its NS and connecting it to the SIS II. Third is a communication infrastructure connecting the CS-SIS and NI-SIS. It will also be used by Member States for the exchange of supplementary information.

The SIS II will enable national competent authorities as defined in Article 21 (3) of the Regulation and Article 40 (4) of the Decision to enter data, access and perform searches in the SIS II directly or in a copy of data of the CS-SIS available in the NS. Member States are allowed to retain a copy of CS-SIS data in their NS for purposes of search. Member States who retain copies of CS-SIS data in their NS are to ensure that the data present in the copies of the data is at all times identical and consistent with the CS-SIS and a search in copies of the data produces the same results as a search performed directly in the CS-SIS.

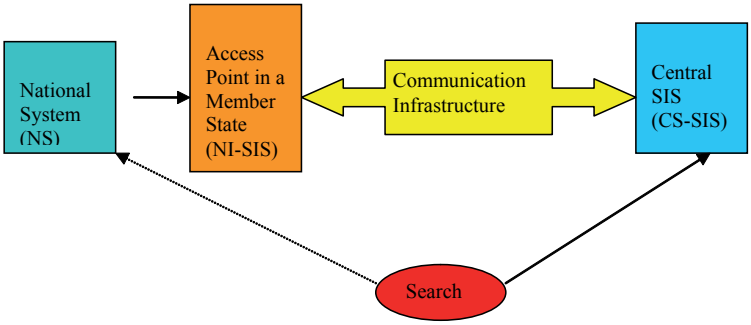


Figure 1: The Technical Structure and Functioning of SIS II

2.3.2. The functioning of SIS II

The main purpose of the SIS is to allow for registration and search of alerts. This purpose is retained in SIS II. However, there is a new function of linking of alerts which is not possible within the current SIS.[14] The effect of linking alerts is to establish relationship between two or more alerts. The interlinking of alerts changes the character of the SIS from a search only system to a search and investigative system. For example, a wanted kidnapper may be linked to a missing child, or an arrest warrant on a suspected car thief to a particular stolen vehicle.[15] While this is welcome for policing purposes, it is not good for individual protection because innocent persons may be mistakenly associated with criminals. For instance where links were to be made between "family members", "gang members" and even "suspected gang members" to one another or "illegal immigrants" to be refused entry with their suspected "traffickers" or between persons subject to discreet surveillance and wanted persons or those to be refused entry, linkage with innocent person may be hard to avoid. The regulation of links between alerts is governed by national law as the SIS II legislation does not make provisions such regulation. In the circumstance the discretion is left to the Member States authorities.

The search process in SIS II is different from that of the current SIS. In the SIS II, search can be done in both the CS-SIS and NS. In the Current SIS search is done in the National SIS (NSIS) only. No search is carried out in the Central SIS (CSIS). The CSIS is an index system and no data are stored in it. In the SIS II, data are stored in the CS-SIS but Member States can decide to store a copy of CS-SIS data in the NS. Where such a copy is stored in the NS, search can be carried out in the NS instead of the CS-SIS, (see figure 1). Member States must however ensure that the NS copy of data is fully updated.

2.4. Control Authorities

2.4.1. SIS II National Office and SIRENE

SIS II national office is designated by Member States and its purpose is to ensure that competent authorities' access to SIS in accordance with the Decision and Regulation. The SIRENE is national authorities designated by Member States with the responsibility of ensuring the exchange of all supplementary information. The authorities have also the responsibility to verify the quality of

14 Article 46 of the proposed Decision and Article 26 of the proposed Regulation

15 Hayes, Ben, SIS II: fait accompli? Construction of EU's Big Brother databases underway. Statewatch Analysis, May 2005. p. 5

the information entered into the SIS II and as such they have they have access to data processed in the SIS II. It seems that the SIS II authorities and SIRENE authorities are to be located in the same SIS II national office. The clear reference of the SIRENE authorities in both the Decision and the Regulation means that the legal basis of the SIRENE is grounded on these two instruments and therefore no longer in doubt as it was in the Schengen Convention before the amendments. The instruments are explicit that the SIRENE is a human interface and not technical at all. Nevertheless, the SIRENE authorities will use the SIS II communication infrastructure for exchange of supplementary information. The role of the national office and SIRENE seems to be clearly defined in the SIS II proposed legislation unlike in the current SIS law.

2.4.2. The Commission

The Commission is responsible for the operation and management of the SIS II. This entails, in particular, the maintenance work and technical developments necessary for the smooth functioning of the system. The Commission must ensure that the SIS II functions on a 24 hours a day, 7 days a week basis. It also has responsibility of keeping data logs for the Central system.

The responsibility for operation and management of the current SIS is vested on France, a Member State. In SIS II, the Commission therefore takes over responsibility from the French authorities as the SIS II is regarded as an agency of the EU. The Commission has also responsibility on another European Union system, the Eurodac, and it is also to acquire responsibility over the Visa Information Systems.

The Commission is assisted by an advisory Committee composed of the representatives of the Member States and chaired by the representative of the Commission. The role of the Committee is to give legislative advice to the Commission by way of opinions.

2.4.3. National Data Protection Authorities

Similar to the current SIS law, Member States national data protection authorities have the responsibility of monitoring the lawfulness of the processing of SIS II personal data on their own territories including the exchange and further processing of supplementary information. For instance, they have the right to access the logs for purposes of monitoring the lawfulness of data processing and to ensure the proper functioning of the system, including data integrity and security. Similar to the current SIS law, an individual has the right to ask the supervisory authority to check the lawfulness of data processing performed in the SIS II concerning him.

2.4.4. The European Data Protection Supervisor

Under both the Decision Article 53 and the Regulation Article 31 the European Data Protection Supervisor (EDPS) has the responsibility to monitor that the personal data processing activities of the Commission are carried out in accordance with the law. For example, the EDPS has the right to access the data logs in order to monitor the lawfulness of the personal data processing operations performed by the Commission including data security. The EDPS has replaced the Schengen Joint Supervisory Authority (JSA) in the current SIS law. It is interesting that the Decision, which is a third pillar legislation, has adopted the EDPS as the supervisory authority. However, the access to and further processing of SIS II personal data by Europol and Eurojust will be supervised by Europol and Eurojust supervisory authorities, Article 53(2) of the Decision. The implication of these changes for data protection is discussed later in 2.4. below.

2.5. Exchange of Supplementary Information

Exchange of supplementary information in the current SIS occurs when there is a positive hit and the authorities concerned require further information in order to fulfil the action required.[16] In SIS II, the exchange of supplementary information for purposes of consultation and informing each other can be requested any time while entering an alert, following a hit, when the required action cannot be taken, when dealing with the quality of SIS II data and compatibility of alerts as well as for the exercise of the rights of access.[17] Instances of exchange of supplementary information are expanded meaning that much more personal data will be exchanged under SIS II than in the current SIS. Member States are to exchange supplementary information through the SIRENE authorities via the communication infrastructure between the CS-SIS and the NI-SIS. Detailed rules for exchange of supplementary information are to be adopted in accordance with the procedures laid out in the legislation. The rules will be published in the SIRENE Manual. The SIRENE Manual is to replace the current SIRENE Manual.

16 SIRENE Manual p. 4

17 See Article 8 both the proposed Decision and proposed Regulation

2.6. Data to be entered in SIS II

2.6.1. Alerts to be entered

Personal data is entered in the SIS if an alert on the person concerned is entered. This also applies to data entered in the SIS II. The old alerts issued under the current SIS law are retained in the SIS II legislation. But two of the alerts have also been revised: alerts on extradition Article 95 and alerts on refusal of entry to foreign nationals Article 96 of the Schengen Convention. Another difference is that the alerts are allocated different legal basis. The alerts concerning judicial and criminal co-operation are allocated to the Decision. The alerts concerning immigration and border entry are allocated to the Regulation.

The Decision regulates the issuance of the following alerts:

- Alerts in respect of persons wanted for arrest and surrender or extradition, Article 15;
- Alerts on persons to ensure protection or prevent threats, Article 23;
- Alerts on persons wanted for judicial procedure, Article 27;
- Alerts on persons and objects for discreet surveillance or specific checks, Article 31;
- Alerts on objects for seizure or use as evidence in criminal proceedings, Article 35.

The first change to the alerts involves alerts relating to extradition data. European Arrest Warrant data are issued as alerts in the SIS II under alerts on arrest and surrender and extradition. This means the scope of these alerts is expanded and will also provide for inclusion of data related to the warrant or extradition request in the SIS II.

The proposed Decision lays down conditions for issuance of each category of alerts in the relevant provision of the category of alerts. For alerts concerning discreet surveillance or specific checks on persons and objects, the collection and exchange of supplementary information is permitted, Article 32. The competent authorities of the Member States which carry out border checks or other police and customs checks within the country may collect and communicate to the authority issuing the alert all or some of the following information:

1. The fact that the person for whom, or the vehicle for which an alert has been issued has been found;
2. The place, time or reason for the check;
3. The route and destination of the journey;

4. The persons accompanying the persons concerned or the occupants of the vehicle;
5. The vehicle used;
6. Objects carried;
7. The circumstances under which the person or the vehicle was found.

Only one type of alerts is regulated by the Regulation namely alerts issued in respect of third country national, for the purpose of refusing entry, Article 15. The alerts under Article 15 are issued on basis of a decision defining the period of refusal of entry taken by the competent administrative or judicial authorities of a Member State. The alerts are issued only on the following cases:

a. if the presence of the third country national in the territory of a Member State represents a serious threat to public policy or public security of any Member State based on an individual assessment, in particular if:
   i. the third country national has been sentenced to penalty involving deprivation of liberty of at least one year following a conviction of offence referred to an Article 2 (2) of Council Framework Decision 2002/584/JHA[18] on the European arrest warrant and the surrender procedures between Member State;
   ii. the third country national is the object of restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the EU Treaty.
b. if the third country national is the subject of a re-entry ban in application of a return decision or removal order taken in accordance with Directive 2005/XX/EC [on return][19].

The second change to alerts is that the regulation has dropped the reference to "national security" from the grounds for registration of "aliens" under Article 96 of the Schengen Convention. However, it has retained reference to "serous threat to public policy and public security" as grounds for registration. However, these terms are still broad and vague. They raise issues of proportionality as persons could be registered on questionable political grounds. It is also worthy to note that the framing of the grounds for registration under this Article does not clearly indicate whether the grounds are exhaustive or not. But it is positive that the regulation grants third country nationals the right

18 OJ L 190, 18.7.2002, p. 1.
19 OJ XX

to a review by or an appeal to a judicial authority against such a decision.[20] However, it is preferable if the grounds were clear and specific but not wide and vague. It should also be clearly indicated that the two grounds provided are exhaustive. As it is, it is difficult to see how the registration of rejected asylum applicants, as has been the practice with Germany under the current Article 96 of the Schengen Convention, can be avoided. It is preferable to clearly state that such registration is not allowed.

Third country nationals will still be subject to discretionary powers of the Member States because they may be entered in the SIS II on grounds of being included on Member States' foreign policy lists of banned individuals. Similarly, persons subject to re-entry bans in accordance with the EC's expulsion Directive may be also be included (despite the fact that the Commission is yet to produce its proposal on this matter).[21]

2.6.2. Compulsory Standard Data

SIS II allows entry of new categories of data that is data which is not allowed in the current SIS. The main change is the inclusion of data on photographs, fingerprints and links between alerts among the compulsory data to be entered in SIS II. In addition, both the Decision and the Regulation have additional specific data for each instrument, different from the common compulsory data items. Under Article 39 of the Decision the following data are to be entered while registering an alert.

a. Surname(s) and forename(s), name at birth and previously used names and any aliases, possibly entered separately;
b. Data and place of birth;
c. Sex;
d. Photographs;
e. Fingerprints;
f. Nationality;
g. Any specific objective and physical characteristics not subject to frequent changes;
h. Whether the person concerned is armed, violent or has escaped;
i. Reasons for the alert;
j. Action to be taken;
k. Authority issuing the alert;
l. In cases of alerts for arrest, the type of offence;

20 Article 15(3) of the proposed Regulation.
21 Peers, Steve, SIS II Proposals, Statewatch Analysis, June 2005.

m. Link(s) to other alerts processed in the SIS II.

Registration of data in items h), j) and l) are specific to the Decision and the registration of these data items is not required by the Regulation.

Under Article 16 of the Regulation the data to be entered is on alerts concerning third country nationals for the purposes of refusing entry. The data are similar to those to be entered under the Decision, but item i) is particular to the Regulation. The Regulation also omits data that are particular to the Decision. The following data are to be entered under the Regulation:

a. Surname(s) and forename(s), name at birth and previously used names and any aliases, possibly entered separately;
b. Data and place of birth;
c. Sex;
d. Photographs;
e. Fingerprints;
f. Nationality;
g. Any specific objective and physical characteristics not subject to frequent changes;
h. Authority issuing the alert;
i. A reference to the decision giving rise to the alert that must be
   i. a judicial or administrative decision based on a threat to public policy or internal security including, if relevant, the decision of conviction or the restrictive measure taken in accordance with Article 15 of the EU Treaty or
   ii. a return decision and/or removal order accompanied by a re-entry ban:
j. Link(s) to other alerts processed in the SIS II.

Registration of item i) is specific for the Regulation as it is not a requirement in the Decision.

The use of the phrase "No more than the following data (…)" in Articles 39 of the decision and Article 16 of the Regulation implies that the list on categories of data is exhaustive. The Member States cannot enter personal data outside the data categories mentioned in the list. The list contains objective data, subjective assessments and sensitive data (photographs and fingerprints). Unfortunately, the prohibition against registration of sensitive data in current SIS law Article 94(3) of the Schengen Convention has been omitted. Accordingly, registration of personal data revealing racial origin, political opinions or religious or other beliefs, as well as that concerning health or sexual belief is not theoretically prohibited, but since the categories of data are restrictive, such data should not be entered. However, it could have been

preferable if the prohibition was incorporated so as to make the prohibition more explicit.

2.6.3. Additional Data for Specific Alerts

The decision further allows additional data on alerts in respect of persons wanted for arrest and surrender or extradition to be entered in the SIS II. Additional data on persons wanted for arrest and surrender are the data referred to in Article 8(1) of Framework Decision 2002/584/JHA and a copy of the original of the European Arrest Warrant, Article 16. The data from the European Arrest Warrant will therefore form part of additional data to be entered in the SIS II. The additional data on person wanted for arrest and extradition under Article 17, are:

a. The identity and nationality of the wanted person;
b. The name, address, telephone and fax numbers and e-mail address of the issuing judicial authority;
c. Evidence of an enforceable judgment or any other enforceable judicial decision having the same effect;
d. The nature and legal classification of the offence;
e. A description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the wanted person;
f. The penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing Member State;
g. If possible other consequence of the offence.

The requirement for registration of additional data will increase the amount of personal data to be entered into and exchanged through SIS II. The SIS II will contain much more personal information than the current SIS.

2.6.4. Additional Data for the Purpose of Dealing with Misidentification of Persons

Both the Decision Article 44 and the Regulation Article 25 permit registration in the SIS II additional data for identification purpose where confusion may arise between the person actually intended by an alert and a person whose identity has been misused. The data to be entered are similar both in the Decision and the Regulation and are the following:

a. Surname(s) and forename(s), any aliases, possibly entered separately;
b. Data and place of birth;
c. Sex;

d. Photographs;
e. Fingerprints;
f. Any specific objective and physical characteristics not subject to frequent changes;
g. Nationality;
h. Number(s) of identity paper(s) and data if issuing.

The data are to be added in order to avoid the negative consequences of misidentification. The requirement is a response to the opinion by the Schengen Joint Supervisory Authority, which had recommended a solution be found regarding individuals whose identity has been usurped.[22] The legislation requires that such information be added into the SIS II with that individual's explicit consent. The information is to be used only for purposes of differentiating the individual whose identity has been misused from the person actually intended by the alert and to allow the individual whose identity has been misused to prove his identity and to establish that his identity has been misused. This inclusion is welcome as it may reduce the risk of a person who is a victim of stolen identity from being identified as the wrongdoer.

2.7. Access to Data by Authorities

Originally, the SIS law only allowed access to data to police and border control authorities. However, access was expanded by amendments to the Schengen Convention to allow access to SIS data to Europol, Eurojust and judicial authorities (will be granted access to all SIS data according to the relevant provisions of the 2004 Regulation[23] and the 2005 Decision[24], from 13 June 2005). In addition, Member States vehicle registration services will have access to stolen vehicle data in the SIS from December 2005.

The SIS II proposed legislation extends access to SIS II data to new authorities. The proposed new Regulation on immigration data is to extend access to asylum and expulsion authorities. Asylum authorities are granted access for the purposes of determining the Member State which has responsibility for asylum applications on the grounds of an illegal stay, Article 18(2) and to take decisions on asylum claim, on grounds that a person is a threat to public order or internal security, Article 18(3). The expulsion authorities are granted access

22 JSA Opinion 98/2 on entering an alert in the Schengen Information system on Individuals whose identity has been usurped (SCH/AUT-CONT (97) 42 REV 2)
23 Regulation 871/2004 amending Schengen SIS rules for immigration data, OJ 2004 L 162.
24 Decision 2005/811 amending Schengen SIS rules for policing and criminal law data, OJ 2005 L 68.

for the purpose of identifying third country nationals staying illegally in the territory so as to enforce a return decision or removal order, Article 18(1). The police will no longer have access to immigration data according to Article 17. This is a welcome exclusion.

The proposed Decision on police and criminal law data does not expand access to SIS II data to any new authorities. It retains the existing rules for various national authorities and Europol. However, for Eurojust there are some changes which require Eurojust staff members to have direct access to SIS II data and not as they do at present through the national members of Eurojust, Article 58. In addition, Eurojust and the national judicial authorities are the authorities with access right to data relating to extradition and European arrest warrants, Article 18(3)&(4). Otherwise, the rest of the conditions for access stipulated in 2005 Decision remain the same for Europol and Eurojust.

The SIS II proposed legislation grants yet more authorities access to SIS II data. But what is worrying is the extension of access to immigration data to asylum authorities. The problem has been expressed by Steve Peers as follows:

> *"In order to apply the Dublin Regulation to determine which Member State is responsible for an asylum application, national authorities need precise information and evidence that a person has been illegally staying on a territory for a specific time. A mere listing in the SIS cannot provide that information. Also, the question of whether a person can be excluded from refugee law (including the EC's asylum legislation) applies a different test from whether a person represents a 'threat to public order or internal security'. A listing in the SIS in accordance with Article 15(1)(a) of the Regulation is manifestly insufficient to this end, particularly since this provision appears to set out non-exhaustive grounds for listing persons."*[25]

The current SIS law does not allow sharing of personal data with third parties. The proposed Decision in Article 48 however opens the possibility of transfer of personal data to third parties. It allows transfer of personal data processed in the SIS II to a third country or to an international organisation where there is an explicit provision for this in EU law. It also allows transfer of the SIS II personal data to third countries or international organisation within the framework of European Agreement in the field of police or judicial co-operation guaranteeing an adequate level of protection of the transferred personal data and with the consent of the Member States that entered the data in the SIS II. This is a clear signal that European countries are willing to exchange personal

25 Peers, Steve, June 2005 supra. p. 15

data for police and judicial co-operation purposes with non-European countries. A good example is the exchange of personal information in the framework of communication of Passenger Names Records (PNR) with USA[26] and other countries such as Canada and Australia.

2.8. Data Protection

2.8.1. General

There are important changes in data protection rules introduced by the SIS proposed legislation, which differ from the current SIS law. Some changes are general and others are specific, that is affecting specific data protection principles. The allocation of the SIS II to different pillars means that there are two sets of general data protection laws protecting personal data in the SIS II. Under the first pillar which is governed by the proposed Regulation, the applicable laws are the EU Directive 95/46 (as regards the national application of the SIS II) and the EC Regulation 45/2001, which sets similar rules governing data protection as regards data processed by the EU institutions including the role for European Data Protection Supervisor.[27] Under the third pillar, which is regulated by the proposed Decision, the main data law applicable is the Council of European Convention of 28 January 1981. The application of two different sets of general data protection laws implies that there will be two levels of protection of personal data, one lower (third pillar) and the other higher (first pillar). This is different from the current situation where all personal data in the SIS are protected under third pillar (lower level) law. In the following sections, I examine the data protection principles in view of highlighting the changes introduced by SIS II legislation.

2.8.2. Security and Confidentiality of Data

Security and confidentiality of data processed in SIS II is provided for in Article 10 of both the proposed Regulation and the proposed Decision. The provision is similar to Article 118 of the Schengen co-operation which deals with security of data in the present SIS. What is new is that Member States are required to take similar security measures in respect of the exchange and further processing of supplementary information.

26 Council Decision 2004/496 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183 of 20.05.2004, p. 83.

27 Ibid. p. 6

As regards confidentiality, it is to apply to all persons and to all bodies required to work with SIS II data and supplementary information. The obligation extends even after those people leave office or employment or after termination of the activities of those bodies. The obligation of confidentiality is new as it is not provided for in the current SIS law. Similar security and confidentiality rules apply for the CS-SIS, Article 13 of both instruments.

Under the current SIS law, Member States are required to record on average every tenth transmission of personal data in the national SIS for the purposes of checking whether the search is admissible. The record is to be deleted after six months. The SIS II proposed law introduces some positive changes. Both the proposed Regulation and Decision in Article 11 respectively provide that Member States are to keep logs for all exchanges of data with SIS II and its further processing. Another new aspect of these provisions is that they give particulars of what is to be recorded. They require that the logs show the date and time of the data transmitted, the data used for interrogation, the data transmission and the name of both the competent authority and the person responsible for processing the data. The duration for the storage of logs has been extended to one year. It is also required that the logs be protected against unauthorised access. Member States are to report to the Commission the findings of monitoring of the logs by competent authorities of the Member States for inclusion in the biannual activity report of the SIS II. Similar rules apply to keeping of logs at the central level (CS-SIS), Article 14 of both instruments.

2.8.3. Quality of Data

Article 24 of the proposed Regulation and Article 43 of the proposed Decision deal with quality of the data processed in the SIS and compatibility between alerts. They place the responsibility for ensuring data quality on the Member State entering the data in the SIS II. The Member State should ensure that the data are processed lawfully and, that they are accurate and up-to-date. It is only the Member State, which entered the data in the SIS II can modify, add to, correct and erase it. Even where another Member State is of the opinion that the data entered in the SIS II are incorrect or have been unlawfully processed, it can only inform and exchange relevant information with the Member State that entered the data to take action. The EDPS is to mediate where the two Member States cannot reach an agreement.

Where alerts in the SIS II relate to the persons with similar characteristics, the Member States are to exchange supplementary information in order to distinguish accurately between the alerts. This is a new requirement that is not contained in the current SIS law.

Another new provision in the SIS II proposed law is that allowing different alerts on the same person to be entered in the SIS II if they are compatible. The rules for compatibility and priority of alerts are to be published in the SIRENE manual. In addition, the Member States are required to review data entered in SIS II at least annually.

The allowing of additional data for the purpose of dealing with misidentification of persons under Article 25 of the proposed Regulation and Article 44 of the proposed Decision are meant to ensure the quality of data and identify the wrongdoers without inconveniencing the victim of identity theft. However, the allowing of creation of links between alerts Article 26 of the proposed Regulation and Article 46 of the proposed Decision may undermine data quality.

Another change that may affect the quality of data negatively is the extension of the duration of data retention. The data storage limits in the current SIS law have been extended for all categories of SIS II alerts. For immigration data, the duration of keeping these data has been increased from 3 to 5 years. The alert shall be erased automatically after five years from the date of the decision to enter them in the SIS II. But it could be erased earlier where the person concerned has acquired citizenship of any Member State or become member of the family of a citizen of the Union or of other beneficiaries of Community law on the right to free movement. The retention duration for data on missing persons and persons wanted for a judicial procedure has been increased from 3 to 10 years. The data are to be automatically erased after 10 years from the date of the decision giving rise to the alert. Further, the retention period for data on surveillance of persons has been extended from 1 to 3 years. After three years the data are automatically to be erased from SIS II. As regards objects possible extensions will be allowed for the first time after the 5 or 10 years. The positive aspect of the data retention rules is that, deleted data will not be kept in the SIS II for one year as required by the current SIS law after deletion. In that circumstance, deleted data may not be retain in any other form. That means that the practice where the deleted SIS data was stored by some Member States in their national systems or SIRENE may not be allowed.

2.8.4. Purpose Principle

Both the proposed Regulation Article 21 and the proposed Decision Article 40 limit the processing of personal data in the SIS II for the purposes and by the competent authorities defined by the Member States in accordance with both instruments. As such access to SIS II data is authorised only within the limits of the competences of the national authority and to duly authorised staff.

Unauthorised and authorisation in excess of the competences of the national authority is prohibited.

According to the Decision, a Member State may change the category of an alert to another where it is necessary to prevent an imminent serious threat to public policy, public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. The new alert replaces the old alert.

The proposed SIS II law also allows copying of personal data in SIS II for technical use. But it prohibits copying of data entered by another Member State into a Member State's own national data files. As such a Member State can only copy the data it has entered into the SIS II to its national data files. However, for the purposes of search, a Member State can copy the entire SIS II data into its national system. Copying of entire SIS II into the national system of a Member State is new as it is not provided for in the current SIS law.

2.8.5. Individual Participation

Article 28 of the proposed Regulation and Article 50 of the proposed Decision introduce a new right of information, which is not found in the current Schengen Convention. The right requires that an individual whose personal data is processed in the SIS II in application of the Regulation and the Decision is informed of:

- The identity of the controller;
- The purposes for processing data;
- The potential recipients of the data;
- The reasons for issuing of the alert;
- The existence of the right of data access and rectification.

The requirement to be informed of the identity of the controller is especially important because it means that the data subject is to be informed which Member State issued the alert. In the current Schengen Convention it is difficult for a data subject to know which Member States issued an alert. However, the right to information is weak as it does not include the obligation to inform individuals about the national or EU supervisory authorities, the right of erasure of data, or the mechanisms of making a challenge, including relevant remedies.[28] It is also not clear whether the obligation to inform is to be carried out prior to registration (especially when the decision is made) or after registration of the alert or when the alert is used to take a decision. In addition, it

28 Peers Steve, June 2005 p. 8

is not explicit whether the right to inform is to be exercised at the initiative of the controllers or at the request of the data subjects.

The right to information under the proposed Regulation is not subject to any exception which is welcome. However, the proposed Decision incorporates an exception in the Schengen Convention. The communication of the information stipulated above is to be refused if this is indispensable for the performance of a lawful task in connection with the data entered in the SIS II or for protecting the rights and freedoms of the individual concerned or of third parties. It is also to be refused during the period of validity of an alert for the purpose of discreet surveillance. The exceptions may render the exercise of the right difficult.

The right of access, rectification and erasure is provided for in Article 29 of the proposed Regulation and Article 51 of the proposed Decision. It entails the right of individuals to have access to, and to obtain the rectification or erasure of their personal data processed in the SIS II. The right is to be exercised in accordance with the law of the Member State before which that is invoked. The fact that the right can be exercised by a data subject in the territory of any Member State gives the person the freedom to shop around as in the current Schengen Convention right of access. When exercised in a Member State that did not issue the alert, the issuing Member State will be given an opportunity to state its position before the concerned Member State communicates to the individual requesting access.

The provisions require the personal data to be communicated to the individual requesting access as soon as possible with a time limit of 60 days from the date of the request of access. The individual is also to be informed of the follow-up to the exercise of the right as soon as possible but not later than 6 months of the request. These requirements are new as they are not found in the current SIS law. They are also positive and desirable.

The proposed Regulation right of access, rectification and erasure does not contain exceptions. This too is new and positive. However, the proposed Decision right incorporates an exception similar to the one in the current SIS law, Article 109(2) of the Schengen Convention. According to the exception, the communication of the information stipulated above is to be refused if this is indispensable for the performance of a lawful task in connection with the data entered in the SIS II or for protecting the rights and freedoms of the individual concerned or of third parties. It is also to be refused during the period of validity of an alert for purpose of discreet surveillance. The exception may render the exercise of the right difficult. The ambiguity found in the exercise of the right to access in the current Schengen Convention will be perpetuated here too.

A right to remedies is also provided under Article 30 of the proposed Regulation and Article 52 of the proposed Decision. The right, which is limited to a person in the territory of any Member State, entitles him to bring an action or a complaint before courts of that Member State in case of refusal of the right of access to or the right to rectify or erase data relating to him or the right to obtain information or reparation in connection with the processing of his personal data contrary to SIS II law. This right is weaker than that found in the current SIS law, Article 111 of the Schengen Convention. It omits reference to the administrative recourse offered by the Schengen Convention. It also drops the reference to the mutual undertaking to enforce final decisions taken by the courts and administrative bodies. The geographical limitation of the right to remedy also weakens the right because in most cases, especially as regards the proposed Regulation, the people affected are foreign nationals who may be outside the Member States' jurisdictions.

2.8.6. Supervision

Supervision and monitoring the processing of personal data in SIS II is to be on two levels: national level and Community level just as in the current SIS law.[29] At the national level, supervision is to be carried out by the existing national data supervisory authorities just as in the current SIS law. However, the Regulation unlike the Decision omits reference to the right of an individual to ask the supervisory authority to check the lawfulness of data processed in the SIS II concerning him. This requirement is part of the current SIS law and it is unfortunate that the Regulation disregards it.

The supervision at the Community level (that is processing of data by the Commission) will be carried out by the European Data Protection Supervisor. The EDPS replaces the Schengen Joint Supervisory Authority for both the proposed Regulation and the proposed Decision. The requirement for the EDPS to monitor data processing within the framework of the proposed Decision is surprising since the Decision is a third pillar instrument. However, the change is welcome as it will improve data protection and monitoring in the third pillar too because the EDPS has more independent and specific monitoring and investigating powers than the joint supervisory authority. However, supervision of the lawful access to and further processing of SIS II personal data by Europol and Eurojust will not be done by the EDPS. The supervisory authorities established by the Europol Convention and the Decision establishing the Eurojust are to monitor the access to and further processing of personal data in SIS II by these bodies. Although this may seem logical, it may complicate

29 See Article 31 of the proposed Regulation and Article 53 of the proposed Decision.

supervisory work at the Community level because of the different supervisory bodies monitoring data processing have diverging powers.

3. SIS II Changes: gains and losses

The foregoing analysis of changes brought about by SIS II proposed legislation indicates clear gains and losses in data processing and data protection. The table below is a summary form of the changes on a strength and weakness perspective which indicates a longer list of weakness than the strength list. In this section, I am going to comment on the changes and how they affect protection of personal data and individual protection in general.

Strength	Weakness
- New legal basis for immigration data - Keeping of all data logs - Data dealing with misidentifications of persons - New Supervisory authority (EDPS) - Right of information - Right of access to data no exception	- Dual legal basis: Council of Europe Convention 1981 applicable - Extension of data retention periods - New data categories - Linking of alerts - Copying of data to the NS - Omission of ban on sensitive data - Data access given to new authorities - Vague and wide data entry criteria - Transfer of personal data to third parties - Right of information vague and with exceptions

Figure 2: Gains and Losses

As regards the legal basis of the SIS II, the proposed Regulation is a welcome improvement to the current SIS law as it creates a new legal basis, in the first pillar, for immigration data. Data protection in the first pillar is considered to offer better protection than in the third pillar on which data protection of the current SIS is based. However, SIS II judicial and criminal data in the proposed Decision is still under the third pillar legal basis. As such, the SIS II has a dual legal basis which might complicate data protection and protection of individuals. Dual legal basis requires distinction between immigration and judicial and criminal data in the application of SIS II legislation. It also means addressing oneself to two sets of laws. It has been the opinion of most SIS commentators,

which I share, that the entire Schengen acquis ought to be transferred to the first pillar. The current changes fall short of this concern.

Both the proposed Regulation and the proposed Decision have the European Data Protection Supervisor as the new supervisory authority at the Community level. This is a good improvement as the EDPS powers are clearly defined and adequate as opposed to the Schengen Joint Supervisory Authority whose powers and budget is limited. Nevertheless I am of the opinion that the mandate of the EDPS is broad and it may not be able to address individual data protection matters adequately as its main concerned is monitoring the application of the SIS II legislation. Individual complaints may not get adequate attention.

The new right of information is a clear improvement as the current SIS law does not contain such a right. Especially, as it requires giving reasons for issuing of the alerts to the person concerned. However, the right has some weaknesses as indicated above. Lack of specification of when the notification is to occur and whether it will be at the initiative of the controller or at the request of the data subject makes the right less useful for a data subject. What the data subject wants to know is when personal data about him or her are being or have been processed by the controller and when a decision has been taken by the authority concerned to enter the data in SIS II. The right should specify when and the mode of exercise of the right. It should be clear when the information is to be communicated to the data subject and at whose initiative: data controllers' or data subjects'.

A clear weakness of the changes is the omission of reference to the prohibition on processing of sensitive data in the current SIS law. Since data protection laws do not incorporate a non-discrimination principle, the ban against processing of sensitive data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life is the closest they come on non-discrimination prohibition. Now that the remote ban is removed, it means that data processing can go on without attention to the principle of non-discrimination.

Linkage of alerts will affect data quality as data of innocent persons may be linked with that of a criminal. Similarly, the proposed extension of data protection retention period may work against data quality. However, the introduction of new data categories especially additional data for the purposes of dealing with misidentification of persons will improve data quality because it will be possible to separate offenders from victims of identity theft.

Alerts on immigration data under the Regulation do not expressly prohibit the registration of asylum seekers whose applications have been rejected in the SIS II. This is a common practice by Germany under the current Article 96 of

the Schengen Convention and has been condemned by the joint supervisory authority and the French Courts.

The Regulation extends access to immigration data recorded in the SIS II to asylum and expulsion authorities. Giving access to asylum authorities may put to jeopardy the application of asylum protection law which requires different criteria from the non-exhaustive grounds for recording immigration data in the SIS II as explained in 2.3.6. above.

The proposed Decision allows full exchange of SIS II data with other non-EU countries and bodies a feature not present in the current SIS law.

4. Conclusion

It is not doubtful that the SIS II proposed legislation has some good improvements on the current SIS law and at the same time some provisions are weaker than the current law. The improvements definitely enhance individual protection. However, it is especially disturbing that the proposed law should be weaker than the current law. This is a clear lowering of protection standards that is unacceptable as it portrays lack of seriousness on individual protection. The least that was expected is an improvement over the current law and not a corresponding movement into the opposite direction.

7 PUBLIC ADMINISTRATION IN THE REPUBLIC OF SERBIA: COMPETENCE, ORGANIZATION AND REFORM

Dejan Jovanovic [1]

Introduction

Basic elements of Serbian public administration, competence and organization, can be analyzed within three global periods and different state forms. The first one relates to the socialist Yugoslavia which existed until 1992 under various names[2]. The middle one began with the emergence of the Federal Republic of Yugoslavia and lasted until 2003. The last one started when the State Union of Serbia and Montenegro was promulgated on March 4, 2003.[3]

Until 1992, both Yugoslavia and Serbia, had a highly decentralized system of government, in which the municipality represented the basic political and territorial unit. It was the so-called "communal system" with a presumption of power in favor of municipality.[4] It was municipality where citizens could directly enforce their rights and obligations toward the state in all fields of activities, unless expressly provided that a certain matter would fall within the competence of a higher unit of government. In another words, the local authorities had power to exercise all activities of state administration, except those

---

1 Researcher at the Institute for Legal and Social Research, Faculty of Law, Nis. Guest at NRCCL/SITAS Winter 2005

2 Democratic Federal Yugoslavia (DFJ) was promulgated on August 10, 1945 which was followed by Federative People`s Republic of Yugoslavia in November 29, 1945 and was succeeded by Socialist Federal Republic of Yugoslavia (SFRJ) on April 7, 1963. The last one, Federal Republic of Yugoslavia, came into existence on April 27, 1992. More on history of Yugoslavia is available on the following page: http://www.gov.yu/start.php?je=e&id=6.

3 The latest of state forms, which included Republic of Serbia, is consisted of two former republics of the Socialist Federal Republic of Yugoslavia (and Federal Republic of Yugoslavia), which are Serbia and Montenegro.

4 This system has been characterized by: a broad range of local self-government competencies including those of economic and territorial defense (which were unique in the world!), almost complete financial autonomy of the local self-government units and a very involved system of administrative and executive organs structured as the Republic and Federal (Yugoslav) governments and each of them being in charge of separate competencies.

that were expressly preempted by the laws for the larger units of government (provinces, republics, federation).[5]

While the rest of the republics of the former Socialist Federal Republic of Yugoslavia have proclaimed their independence, at the beginning of 90`s, Serbia (together with Montenegro) promulgated new Constitution[6] and regulated the public administration in a completely different manner than it was earlier (i.e. as a centralized system). Since than, the concentration of powers in favor of the republic member of the federation (while Serbia was in FRY) and member of the State Union (while it is in Serbia and Montenegro) was/is the main feature.[7]

Based on this knowledge, Serbian public administration is dominantly competent which shows, on the other hand, the position of the local self-government. The competence of the local self-government is limited to very few fields. The basic feature of the Serbian legislation is the centralization of all operations of state administration on the republic level. This relationship could be designated as a strict subordination of local administration to the state administration when applying republic laws.

1. Republic administration

1.1. Competence

According to relevant provisions of the Yugoslav constitutional documents, it is primarily seen that administrative competence was in favor of member republics.[8] All administrative matters that were not (explicitly) excluded by the mentioned documents, were matters to the competence of the Serbia.

Present situation talks for exactly the same. Generally, agencies and organizations of the Republic of Serbia can be entrusted with the law enforcement

5 Thus, the municipal authorities dealt with matters of education (with exception of universities), police, finance, culture, health, defense, commerce, public utility services, traffic, etc. Almost all traditional state functions were conducted on the local level not excluding the typical tasks and activities of the local government.

6 Enacted by the Parliament of the Republic of Serbia on September 28, 1990.

7 This means that the competence of the federal administration was (and still is) limited only to the fields that were/are explicitly envisaged by the (former) federal Constitutions and present Constitutional Charter of the State Union of Serbia and Montenegro (enacted on March 4, 2003). It should be mentioned that fields in question are not numerous.

8 It was the case from the beginning of Yugoslav history after the World War II. This trend, has been particularly made strong, after the enacting the Constitution of SFRJ on February 21, 1974 and introducing some confederal elements.

within the competence of Republic of Serbia, while its state agencies are responsible for the implementing of the entire legislation.

Under the Constitution[9] of the Republic of Serbia, the following matters belong to the competence of the Republic of Serbia:

- sovereignty, independence and territorial integrity of the Republic of Serbia and its international position and relations with other states and international organizations;
- realization and protection of freedoms and rights of man and citizen; constitutionality and legality;
- defense and security of the Republic of Serbia and of its citizens; measures to cope with state of emergency;
- property and obligation relations and the protection of all forms of ownership; legal status of enterprises and other organizations, their associations and chambers of economy; the financial system; the system in the spheres of economic relations with foreign partners, market, planning labor relations, protection at work, employment, social security and other forms of social security as well as other economic and social relations of public interest;
- the system of protection and advancement of human environment; protection and promotion of plants and animals;
- the system in the spheres of health care, social protection, war veterans' and disabled persons' care, social care for children and young people, education, culture and protection of cultural monuments, physical culture, social and public information;
- the system of public services;
- control of the legality of disposal of resources of legal entities, auditing of public expenditures and the way of uniform organization of such affairs; collection of statistical and other data of public interest;
- basic goals and directions of the economic, scientific, technological, demographic, regional and social development, the development of agriculture and rural areas; organization and the use of space; policy and measures to guide and promote development, including the development of under-developed areas; commodity reserves:
- financing the realization of the rights and duties of the Republic of Serbia as established by the Constitution and law;
- organization, jurisdiction and work of republic agencies;

9 Art. 72.

- other relations of interest for the Republic of Serbia in accordance with the Constitution.

According to article 135 of the Serbian Constitution "rights and duties that Serbia has under her Constitution and which are supposed to be carried out on the federal level, having been placed there by the federal Constitution itself, shall be carried out in accordance with the federal Constitution".[10] Besides, if the federal acts or acts of the other republic infringe the equal status or some other interests of the Republic of Serbia, her agencies are competent to act in order to protect its interests.[11]

1.2. Organization

Ministry is the only administrative division of the republic administration which is expressly provided by the Constitution.[12] Ministries may have administrative agencies within its internal structure which are to be founded by the statute, if the nature and character of the tasks and activities thereof, as well as the necessity for their independent and expedient work can justify their creation. Until recently, there were no such agencies at all due to the fact that the authority vested in ministries has been distributed to various internal sectors headed by minister assistants.[13]

In accordance with the competence of the Republic of Serbia, number of its ministries is significantly higher comparing to the administration of the State Union.[14] According to the Law on Ministries there are 17 ministries for the following areas: interior affairs; finance; justice; public administration and local self-government; agriculture, forestry and water resources management; economy; mining and energy resources; capital investment; trade, tourism and services; international economic relations; labor; employment and social po-

10 Due to fact that the Constitution of Serbia has been enacted before the Constitutional Charter in 2003, it is reasonably that there is overlapping between the Republic and federal competence with respect to certain matters.

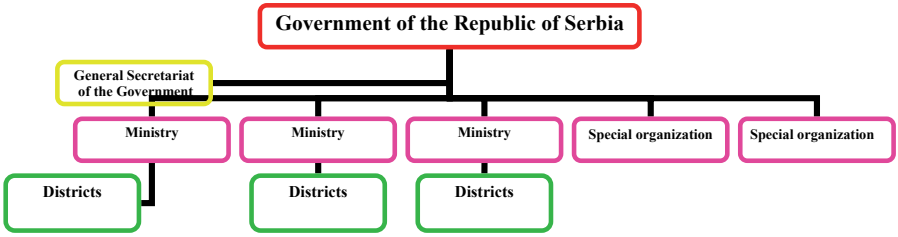
11 Inspite the fact of having legal right to form its own army or ministry of defense as well as ministry of foreign affairs (which it might have under the enumerated competencies), Serbia did not take such a chance. Serbia`s official attitude is that all these matters are supposed to be carried out on the federal level.

12 Art. 94 of the Constitution.

13 The first one was established on November 19, 2001 by the Law on the Agency for development of small and medium enterprises, Official Gazette of the Republic of Serbia, 65/01.

14 Besides the President of the Serbia and Montenegro, who is in the same time President of the Council of Ministers, there are just five ministers for: foreign affairs, defense, international economic relations, internal economic relations and human and minority rights.

licy matters; science and environmental protection; education and sport; culture; health; religion and for diaspora.[15]



Scheme 1: Relations between the Government and central administration in the Republic of Serbia

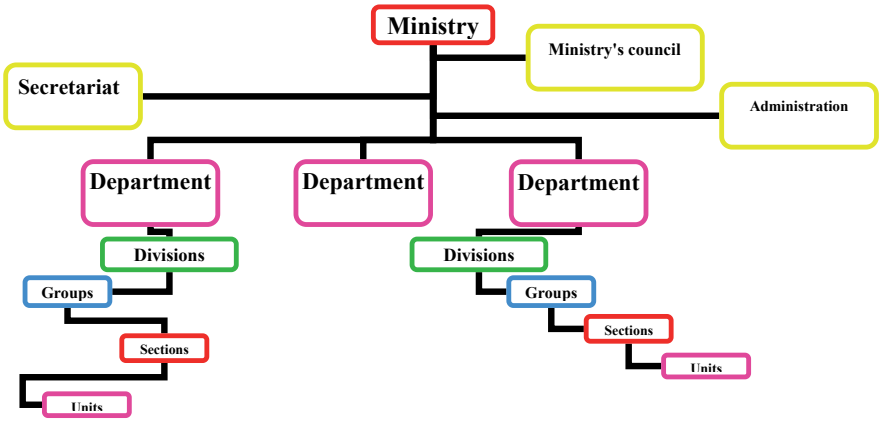
Apart from ministries, which are the traditional forms of administrative agencies exercising executive power, there are also administrative organizations in the Republic of Serbia. Strictly speaking, the Serbian Constitution (art. 94 para. 4, 5, 6) does not include administrative organizations but "special organizations"[16]. As administrative organizations, special organizations perform professional duties supporting the functioning of the government. From this point, there has been no substantial change, since these organizations remained the same and their legal status has not been considerably modified. Special organizations are to be founded for certain professional and public administration activities and tasks. Two new types of the administrative organizations were introduced: secretariats and administrations, which are the terms formerly

15 See, Law on Ministries, Official Gazette of the Republic of Serbia, 19/04 and 84/04. Additional information available with the Proposal of the Law on Government of the Republic of Serbia.

16 There are seven special organizations: the Republic secretariat for legislation, the Republic institution for development, the Republic institution for statistics (formerly on a federal level known as statistical office), the Republic hydro-meteorological institute, the Republic institution for land surveying, the Republic bureau for the property of the Republic of Serbia, Agency for informatics development and Internet, Agency for infrastructure development of local self-government, Serbian investment and export promotion agency and Center for mine detection. For more see, art. 21 of the Law on Ministries.

used for administrative state agencies only.[17] Such administrative organizations did not exist before and they have not been introduced to the federal level either. Beside them, the regulations also introduce traditional administrative organizations, such as institutions and bureaus.

Ministries, as well as special organizations are divided into departments which perform operations in certain branches of executive power. Usually, departments are established to group certain duties and affairs. In multi-portfolio ministries (ministry for science and environmental protection, for example), a department covers one of the portfolios (i.e. for environmental protection). When discussing "single-portfolio" ministries (ministry of finance, for example) departments are organized to group together similar affairs (i.e. macroeconomic and fiscal analysis, public finances and budget policy, treasury, budget inspection and audit, fiscal system, property legal issues, finance system, customs system and policy, foreign currency inspection, secondary infractions proceedings).



Scheme 2: Ministry internal organization in the Republic of Serbia

17 The following ministries have administrations: ministry of finance (tax administration, public payment administration and customs administration (art. 4 of the Law on Ministries)) ministry for agriculture, forestry and water resources management (administration for the furriery (art. 7 para. 2), administration for vegetation protection (art. 7 para. 3), Republic directorate for water resources (art. 7 para. 4) and administration for forestry (art. 7 para. 5)), ministry for trade, tourism and services (the Republic bureau for commodity reserves, art. 11 para. 2), ministry for science and environmental protection (administration for the environmental protection, art. 14 para. 2) and ministry for education and sport (administration for sport, art. 15 para. 2).

Internal organization of the ministry and department goes through divisions to groups. The groups are divided into sections and the whole process ends up with the units.[18] At all the named level of organization it is possible to set-up a special advisory post filled by one person, but technically treated the same as an organizational unit. In all the ministries there is a general department called "secretariat" which is in charge of general and common affairs in the ministry (personnel, general administration, procurement, minister's office, welfare, etc.). It should be noted that minister is *de jure* powered to reorganize a ministry, but such by-law on ministry internal organization must be approved at a governmental meeting.

Another characteristic of the ministries is a special body called a ministry's council. It is an advisory (a special think-tank) body consisted of academians, professionals, distinguished public figures who can advise minister on policy and technical issues. In multi-portfolio ministries usually there are a couple of them depending on how many portfolios the ministry covers. Although the body has an advisory role, it can be sometimes quite powerful, since it is usually a "politician-free area" where leading public figures take part.

A ministry is headed by a minister elected by parliament and the deputy of the minister is appointed by the government. Technically, both of these officials are pure political appointees.[19] The secretary to the ministry heads the secretariat, who, as a senior civil servant, provides necessary technical advice for the day-to-day functioning of the ministry. The department head holds the title of an assistant minister. Sometimes it is possible that the deputy minister can be in the same time and head of the department. According to the law ministers assistant is fully responsible[20] for law enforcement and application of governmental policies within its department.

Administrative agency is headed by a director (or rarely a secretary, i.e. only in the case of the secretariat for legislation), who has a deputy. Departments are headed by assistant directors. In the special organizations the duty of the permanent secretary does not exist. Formally, deputy ministers, secretaries and assistant ministers, along with directors with their deputies and assistants (a

18 In some ministries a special division can be established and directly linked to the minister, without departmental affiliation.

19 It may occure (very rarely!) that a deputy minister can be a distinguished administrator and/or professional, not politically affiliated with (or even backed by) the ruling party (or ruling coalition).

20 While minister has all political responsibility, assistant minister is technically/professionally responsible.

deputy secretary and assistant secretaries in the case that a special organization is headed by a secretary) create a group of senior civil servants[21].

According to the Serbian administrative laws[22], there are three classes of the civil service, members:

- "Elected personal", i.e. ministers who are always, at the far end, accountable to Parliament, which elected them to the post.
- "Appointed personal" includes the members of service who have been appointed by the government for four years, but any change of government may cause changes amongst deputy and assistant ministers.[23]
- "Employed personal" (which includes professional and technical staff, so called "ordinary" or "career civil servants", up to the rank of "adviser to the minister")[24].

2. Administration of the Autonomous Provinces

The status of the province administration is highly determined by its new status in the constitutional system of Serbia.[25] A province is a unit of territorial autonomy entrusted with less authority after the Republic of Serbia had im-

21 Instead of this one, in more colloquial use is the term "appointed personnel" for making the difference to "elected"or "employed personnel".

22 At the first place it understands the Law on employment relations in the public administration. See, the documentation list of it at the end of this paper.

23 In last couple of decades it was the case that senior civil service corps has been heavily changed. Usually, just after the election, one of the first decisions of each minister was to establish his/her own executive team. Inspite the claims of some academians (Rabrenovic, for example) that "this pattern cannot be applied to the main ministries" such as ministries of finance, internal affairs, education etc, recent developments talks for opposite. Naimely, minister of education and sport in the Government of the late Prime Minister Djindjic, has employed 200 servants (among them fifteen of his advisers, assistants and deputies!). This was, in the time when occurred, 50% of the total ministry personal. More on this is available at: http://www.politika.co.yu/cyr/default.asp.htm.

24 In a few rare cases a civil servant can be appointed as a "republican adviser" (in the secretariat of the Government or the secretariat to the President of the Republic), which is hierarchically under the assistant minister position.

25 Taking into account the current situation in Kosovo and Metohija, we are going to analyze here only issues related to the Autonomous Province of Vojvodina. There is only one type of the administrative agencies envisaged by the Decision on Public Administration of the Autonomous Province of Vojvodina, which is the secretariat of the Province. The legal framework allows the establishment of administrative organizations in the Province, but the aforementioned Decision has not envisaged any. There are seven secretariats of the Province: for economy; agriculture; culture and education; information; health, labor and social policy; finance; realization of national minority rights, administration and general enactments (there are two special services within this secretariat: Service for the realization of minority rights and the Translation service).

posed direct rule. The provinces are entrusted only with the rights explicitly provided in the Constitution (art. 109), which amounts to: regulating some matters (not all of them) in the areas of: culture; education; official use of the language and alphabet of the national minority; public information; health and social welfare; child welfare; protection and advancement of environment; urban and country planning; and in other areas established by law.[26] Also, the important feature that sheds light on the status of a province is that provinces enforce laws, other regulations and general enactments of the Republic of Serbia, whose enforcement has been entrusted to the agencies of the autonomous province, and pass regulations necessary for their implementation if so provided by the law. The Republic of Serbia may entrust by a law an autonomous province with the performance of specific affairs within its own competencies.

The province has no legislature so it cannot promulgate laws. The Statute of the Province is the highest legal act of this territorial unit, while the Assembly of the Province has power to enact decisions. The agencies of the autonomous province are its assembly, executive council, and agencies of administration.

The Republic of Serbia has entrusted by means of law the autonomous province with the performance of specific affairs within its own competencies, in accordance with the Constitution. In 1992 the Government of the Republic of Serbia delegated the performance of certain affairs within the competence of five ministries to the administration of Province by the Decision on Delegating the Performance of Public administration Matters to the Administration of the Autonomous Province of Vojvodina. Since this is the delegation of powers to the administration of the Province, the administrative officers of the Province are accountable to the ministries. If there is a request coming from a ministry, the administration of the Province has duty to prepare information and reports, and furnish data and facts in connection with the performance of delegated powers.

3. Districts

Districts comprise several municipalities which are considered to be territorial divisions placed between central and local levels forming a link among

26 Law on determing certain competences of the Autonomous Provinces, Official Gazette of the Republic of Serbia, 6/02.

them.[27] As a territorial units districts are bringing together the departmental bodies of certain administrative agencies (ministries and other state agencies and organizations) in a single administrative center for the particular area (so-called de-concentrated administrative agencies). In order to exercise their jurisdiction and perform certain activities in regions where their principal seats are not located, ministries can form organizational units in certain areas determined by the Government. These departmental bodies for a designated area taken together form the administrative center of the state administration for particular area, while these areas are called districts with seats determined by the Government.

Districts as a middle level government includes administrative territorial units of the state entrusted to conduct regional policy, the exercising of state powers, the implementation of state policy on the local level and harmonization of national and local interest. Taken as territorial branches of the Republic administration, districts have neither autonomy nor elected bodies.[28] The district public officer[29] is appointed for a four-year term by the central government aimed to coordinate the work of government agencies within the region and their interaction with local authorities. In particular, he/she ensures the implementation of state policy, protects state property and state interests within the district, law and public order and exercises administrative control[30]. The district public officer coordinates the work of government agencies within the region and their interaction with local authorities. The district head issues

27 By the Law on territorial organization and local self-government, adopted on July 24, 1991 the municipalities, cities and settlements make the bases of the territorial organization. Further more, by its Executive order on the conduct of affairs of ministries and special organizations in places other than their place of seat of January 29, 1992, the Government of the Republic of Serbia (hereafter: the Government) defined the state administration affairs that shall be run by the competent ministries out of their seats, within the districts as regional centers of state authority. The Government formed 29 districts as a new type of territorial divisions in which state authority is decentralized for the purpose of executing state power in legally defined areas and which pursues effective regional policy. These divisions do not possess original constitutional status, since the Constitution does not provide for their existence. This is why they have derivative character in a constitutional sense. Since they are not expressly envisaged by the Constitution of the Republic of Serbia, they belong to some sort of non-constitutional category, although they are not unconstitutional.

28 Concerning intergovernmental relations, there is a strict division between the powers, responsibilities and tasks of central government, district and local self-government according the law.

29 Similar to the function of the regional governor but not exactly the same.

30 The district public officer exercises control over the legality of the acts as well as actions of bodies of local self-government unit and may cease execution of unlawful acts of municipal councils and refer them to the appropriate court. In addition, there is a power of rescinding unlawful acts of municipal mayors and other bodies of the local self-government unit.

ordinances within the scope of powers conceded to him/her and is aided by the district administration.

District, like local self-government unit, can also have independent administrative officers. Choice between two options: independent administrative officers and departmental agency will depend solely on the nature and character of tasks and activities thereof. There is also a possibility for two or more districts to perform some of the affairs together by providing the performance in the capitol of one of the districts.

Unless the ministries and special organizations are expressly authorized, they are not allowed to fully exercise their jurisdiction within the districts. The matters they are usually authorized for are the administrative procedure (first and second instance) and the exercise of administrative control. They are as follows:

- Administrative control;
- Administrative procedure (first instance);
- Administrative procedure (second instance) when the first instance administrative procedure is vested in municipalities, enterprises, institutions and other organizations by means of law;
- Control over the public administrative activities when delegated to the local administrative agencies;
- Professional supervisory control over the enterprises, institutions and other organizations;
- Other matters that ministries and special organizations are competent for, except for the analytical and programming matters, and the advancement of certain matters which belong to ministries and special organizations.
- Regulations on the organization and systematization of each ministry and special organization contain precise tasks and activities which are to be conducted within the district.

4. Local self-government

4.1. Competence

During the last decade of the 20th Century, Serbian law makers were in between of rejecting of the communal system[31] of local self-government and the centralization which gives rise to the entire organization of state authority caused disappearing of municipality's previous importance. Current system, compared to the previous one when a municipality was the most important territorial and political unit, which exercised the function of state power for its own benefit, is completely different. The former assumption of state power in favor of municipalities has been replaced by entrusting the state power solely to the central state agencies of the Republic.

The system of local self-government is exercised in a municipality, city and the city of Belgrade.[32] It should be noted that a municipality is a basic unit of local self-government. Regardless of the fact that city and municipality are distinct categories, city exercise the functions of a municipality.[33] Nevertheless, they are entitled to larger financing funds. Apart from revenues that belong both to cities and municipalities[34], cities are entitled to extra 10 % of the turnover tax on products and services collected in the city, which is designated for financing governmental expenditures of the Republic of Serbia.[35]

---

31 This system did not produce good results in practice because, at one side, it created extremely high level of local government autonomy, and on the other, significantly reduced the beneficial influence of the state in the process of coordination of economic activities. Thus, the opportunity for any municipality to carry out its own economic policy led to many parallel economic enterprises being established both in the Republic and in the Federation, and many of them undertook measures contradictory to those of the central authorities. For example, some taxes were decreased by republic or federal ministries in order to stimulate exports and at the same time communal taxes were raised, annulling the positive effects of the former activity.

32 For the purpose of this paper, and in compliance with the art 1. par. 2 of the Law on local self-government, Official Gazette of the Republic of Serbia, 9/02, we shall use the term "local self-government units".

33 Art 21 of the Law on local self-government, also, states that "the city shall be the territorial local self-government unit consisting of two or more city municipalities."

34 According to the Constitution and law(s), local self-government unit fund its needs from own income, as well as from state subsidies. The law states which taxes and fees represent the local self-government unit income.

35 According to the mentioned Law, City of Belgrade is entitled for additional 15% of the turnover tax on products and services collected in the City of Belgrade, which is designated for financing governmental expenditures of the Republic of Serbia.

As a legal entity[36], local self-government unit own assets, has its own budget, personal and financial independence and it may do business, collect local taxes and fees.[37] A municipality, neither city, has no state functions and serves only for purposes of local self-government. However, in selected areas where it is more advantageous for the state, self-government can execute transferred scope of the state administration operations.[38] In that respect, there are two types of the local self-government units` powers[39].

The first one comprises the original powers (competencies) of the local self-government unit. These are the affairs of vital interests for citizens, as determined by the Constitution, law and a statute of a local self-government unit. Original competencies include:

- make development plans and programs;
- develop city planning projects;
- adopt the budget and final statement;
- regulate and ensure the functioning and development of communal services (water purification and distribution, production and distribution of steam and hot water, local town and commuter transportation of passengers in road traffic, cleaning of towns and settlements, maintenance of landfills, maintenance, spatial planning and utilization of green markets, parks, green, leisure and other public areas, public parking spaces, public

36 Art. 11 of the Law on local self-government.

37 According to discussions which are going on in Serbia at the moment over this question, the local self-government unit budget preparation on an annual basis and its financing through the transfers from the state budget (share on state taxes, special-purpose subsidies) shall be modified in the future. Not just in amount of transferred resources but, primarily, through the changing of the methodology needed for its preparation. This is in compliance with the decentralisation process which, also, includes the change in the field of local self-government funding. The main objective is to strengthen the financial autonomy of local self-government, to increase stability of income base, increase the pressure on more efficient use of own incomes and linking the scope and quality of services provided by territorial self-administrations with tax burden of population. For example, greater power of the local self-government in education is changing the manner of financing. Namely, as the founder of primary schools, municipality receive funds according to criterias mentioned in law (most likely they are: the norm per one pupil, kind, type, size of school etc.). See, the Law on self-government, art. 5, 19, 77 – 104 as well as following links: http://www.skgo.org/, http://www.beograd.org.yu/, http://www.nis.org.yu/, www.gradnovisad.org.yu/, www.kragujevac.org.yu/ as well as daily newspapers: http://www.danas.co.yu/ and http://www.dnevnik.co.yu/.

38 Art. 2 of the Law on local self-government.

39 Basically, Law on local self-government states the municipal powers in art. 18. In addition art. 22 states that "the city shall perform the original responsibilities of the municipality, as well as the delegated responsibilities within the rights and responsibilities of the Republic and the forms of Territorial Autonomy."

illumination, maintenance of cemeteries and burials, etc.) as well as organizational, financial and other conditions for their functioning.
- ensure the maintenance of residential buildings and the safety in the utilization thereof, and determine the amount of maintenance fees;
- carry out the eviction procedures of illegitimate tenants from flats and common facilities in residential buildings;
- develop construction land development programs, regulate and provide for the development and utilization of construction land, determine the amount of charges for the development and utilization of construction land;
- regulate and provide for the utilization of business premises managed by the municipality, determine the rents for the utilization thereof, and supervise the utilization of business premises;
- take care of environmental protection, make programs for utilization and protection of natural resources and environment, *i.e.* local action and recovery plans, in accordance with strategic documents and its interests and specifics and determine the amount of special charges for the protection and improvement of the environment;
- regulate and provide conditions for the construction, rehabilitation and reconstruction, maintenance, protection, use, development and management of local and non-categorized types of roads as well as streets in settlements;
- regulate and provide special conditions and the organization of taxi services;
- regulate and provide for waterway line transport within the territory of the municipality, and determine the parts of the riverbank and water area which can be utilized for the construction of water constructions and floating facilities.
- set up goods reserves, and determine their volume and structure with the consent of competent Ministry, for the purpose of fulfilling the needs of local population;
- establish institutions and organizations in the field of primary education, culture, primary health care, physical culture, sports, child and social welfare, and tourism, monitor and provide their functioning;
- organize activities related to the protection of cultural assets of local significance, encourage the development of cultural and artistic amateur activities, and provide conditions for the work of museums and libraries, and other cultural institutions established by the municipality;
- regulate and organize protection against the elements and other disasters, protection against fire and create conditions for the purpose of eliminating and/or alleviating the effects thereof;

- prepare the basic guidelines for protection, utilization and development of agricultural land, and provide for the enforcement thereof, define the areas affected by erosion, regulate the utilization of pasture land, and decide on their conversion into different agricultural purpose;
- regulate and define the manner of utilizing and managing springs, public wells and fountains, define water-supply conditions, issue water-supply approvals and permits for the facilities of local significance;
- provide adequate conditions for the purpose of preserving, utilizing and improving the areas with natural curative properties;
- encourage and attend to the development of tourism within its territory and determine the amount of the sojourn fee;
- ensure the development and improvement in hotel and restaurants services, handicrafts and trade, regulate the working hours and location for the performance of such activities and provide other conditions for their functioning;
- use state-owned property, with due diligence in preserving and expanding thereof;
- regulate and organize activities related to the breeding and protection of domestic and exotic animals;
- organize activities related to the legal protection of rights and interests of the municipality;
- establish bodies, organizations and services to meet the needs of the municipality, and regulate their organization and operation;
- encourage and support the development of cooperatives;
- organize, as needed, legal assistance services for citizens;
- ensure the protection and exercising of personal and collective rights of minorities and ethnic groups;
- specify the languages and alphabet of minorities to be officially used on the territory of the municipality;
- provide public information of local significance;
- prescribe the offences resulting from the violation of municipal regulations;
- establish inspection services and ensure respective supervisory activities regarding the application of regulations, and other general by-laws within the municipal authority;
- regulate the organization and work of mediation committees;
- prescribe and provide the use of the name, coat of arms and other symbols of the municipality;
- engage in other activities of direct interest to the local population in accordance with the Constitution, law, and the statute.

The second group comprises powers of the local self-government unit vested in it by the Republic of Serbia or Territorial Autonomy. These may entrust by means of law the performance of "specific responsibilities within the rights and responsibilities" to a particular local self-government.[40] Such a delegation of powers will take place if the efficiency and expediency in meeting the needs of citizens and realization of their rights and duties are going to be accomplished thereby.[41] According to the law, the local self-government will be engaged in specific activities having the status of delegated responsibilities related to the inspection in the field of trade in commodities and services, agriculture, water-supply and forestry and other inspection activities in accordance with the law.[42]

It should be pointed out that local self-government units perform their duties in various ways: independently and in a (voluntary) cooperation (interior or international[43]) among local self-governments units. An interior form of cooperation among local self-government units is their membership in the "Permanent conference of the cities and municipalities". Most of the local self-government units in Serbia are its members. The supreme aims of the Conference are: development and protection of local self-government, connection and cooperation of the municipalities and cities aimed to fulfilling their common interests and establishing and developing cooperation between the municipalities and cities with international municipalities and cities as well as

40 Art. 113 of the Constitution and art. 19 par. 1. of the Law on local self-government.

41 These delegated responsibilities are performed in the name of the state, the state is liable for management of quality of services and funding of such responsibilities depending on their type and volume. It is necessary to add that the transfer of powers to the Serbian local self-government will have to continue in the future particularly in the field of education and primarily healthcare.

42 Art. 20 of the Law on local self-government.

43 This form of the cooperation is in accordance with the art. 10 of the European Charter of Local Self-Government from 1985, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/122.htm and art. 12 of the Law on local self-government. For example, the City of Nis is the member of network of cities, such as: BALCINET (The network of the biggest Balkan cities), South Eastern Europe City Network (which contracting partner is Eurocities organization, available at www.eurocities.org) as well as Energie-Cites, the Association of European local authorities promoting local sustainable energy policy (http://www.energie-cites.org/). Apart from that, Nis participates in Eurobalkan Nis-Sofia-Skopje project and international initiatives such as Conference on Glocalization. One very interesting issue deserves to be mentioned: twinned process with the foreign municipalities. Nis is twinned with the municipalities and cities from: Greece, Bulgaria, Slovakia, Russia, Norway (Saltdal Kommune – Rognan), Germany and Poland. Their cooperation is very often based upon interpersonal and cultural grounds. A delegation from one municipality visits another, establishing personal and sometimes business connections and cooperation in that way. As a rule, they are accompanied by folk-dance ensembles. Information is available at the City of Nis official web-site: http://www.nis.org.yu/.

with the national and international organizations of local government authorities.[44] Apart from this local self-government unit, also, may have a co-operation with businessmen, private sector or establishing joint ventures (for example in waste economy, water economy, maintenance, etc.). For the performance of its duties, it need to establish budgetary and contributory organisations (even to establish partnerships in some cases) and/or contribute by assets to not-for-profit organisations.[45]

Concluding over this part, it will be enough to say that the local self-government unit plays dual role in that respect. At one hand, it directly enforces local acts, and on the other, it may implement and enforce laws and other regulations of the Republic of Serbia or Territorial Autonomy, when its enforcement is entrusted to it.

4.2. Organization

Unlike the previous system, the current system of local self-government has uniformly organized local self-government units through-out the whole country.[46] The exception to the rule are the capital of the Republic, City of Belgrade, and three other cities, Novi Sad, Nis and Kragujevac, which consists of more municipalities.[47] According to article 21 of the Law, city is a territorial unit of local self-government established by the means of law in whose territory two or more townships may be established. City is a derived territorial unit with competence of a municipality, as determined by the Constitution, which can perform the af-

44 This Conference has various tasks, but among the most important is to discuss any draft of law or any other regulation concerning local self-government issues (still not on a mandatory base). It is a place where local self-government representatives can gather and consult each other on any question concerning either an individual local self-government or many of them. They can even, as a voluntary form of financial transactions among local self-government, lend money to each other usually without any interest. It is, also, a place where conflicts among local self-government may be solved in an informal way. Finally, this Conference cooperates with similar foreign associations and may help Serbian local self-government unit in establishing links with a foreign one. For more on the Conference (or in colloquial use "National Association of the local authorities"), please see, http://www.skgoj.org/publikacije/PDF/Statut%20SKGO.pdf.

45 For example, the City of Nis participates in the Self-Government Reform Program (SLGRP) with the USAID.

46 As of today there are 141 municipalities in the territory of the Republic of Serbia (Kosovo and Metohija excluded).

47 Except for the mentioned cities, which have two levels of self-government, city and municipal wards, in Serbia there is single-level municipal self-government. The distribution of duties, rights and responsibility is stipulated by the Law on local self-government and the statutes of these cities. It is expected that the Law on Capital City of the Republic of Serbia will be soon introduced.

fairs entrusted to it by the Republic by means of law and within its jurisdiction, as well as the affairs determined by means of a statute of the city.

The organization and work of a local self-government unit is regulated by its statute, which is the principal legal act of a local self-government unit, as well as by the decisions and other local self-government unit regulations, provided that they are in accordance with the Constitution and law. It should be underlined that the Constitution and state laws have restrictively framed the competence of a local self-government unit and limited its organizational autonomy.

The bodies of a local self-government unit are as follows: municipal assembly, president of the municipality and municipal council.[48] The same stands for the city level, as well.[49] Compared to previous Law on local self-government, present in force has introduced in April 2004, city major and president of city municipality as directly elected (local) officials. Candidates (i.e. inhabitants), who are having permanent residence on the municipality territory and submit certain number of signatures of the municipality inhabitants, may be proposed by a political party or they may candidate as independent. Officials are elected on the basis of general, equal and direct voting right, by secret voting by voters for the period of 4 years.[50]

The municipal assembly is the principal body of a municipality. It is a representative body composed of "delegates elected by citizens through a direct secret vote, in accordance with the law and the municipality statute".[51] Performing the main functions of local authority, municipal assembly is responsible for the following: adopting the statute of the municipality and the rules of procedure of the municipal assembly; adopting the budget and final statement of the municipality; make the program for the development of the municipality and specific activities; developing the city planning projects and regulating the utilization of construction land; adopting regulations and other general by-laws; scheduling the municipal referendum and the referendum in a part of the municipal territory, adopting proposals contained in citizens' initiatives, and make the proposal of the decision on contribution fee; establishing services, communal public enterprises, institutions and organizations stipulated by the statute of the municipality (supervision of their work is included); appointing and dismissing the management and supervisory board (as well

48 Art. 25 of the Law on local self-government.

49 Art. 46 of the Law on local self-government says "the bodies of the city shall perform the activities prescribed by this Law for the bodies of the municipality, as well as other activities determined by law and the statute of the city".

50 Art. 40 para. 2. Law on local self-government.

51 Art. 26 of the Law on local self-government. When discussing about all the other issues of municipal assembly, see art. 31 - 39.

as the directors) of communal public enterprises, institutions, organizations and services founded by the municipal assembly together with approving their statutes in accordance with the law; electing the chairman of assembly and the deputy chairman of assembly and upon the proposal of the president of municipality electing the municipal council; appointing and dismissing the secretary of assembly; appointing and removing the head of municipal administration (*i.e.* heads of administrations, upon the proposal of the president of municipality); determining municipal fees and other locally generated revenues as provided by law; determining the charges for the development and utilization of construction land; adopting the by-law on the municipality's public debt; regulating the working hours of hotels and restaurants, trade and handicraft facilities; giving an opinion on the urban plan on the level of the Republic, Territorial Autonomy and District; giving an opinion on the laws regulating the issues of interest to the local self-government; initiating the proceedings for the protection of local self-government rights before the Constitutional Court; giving consent on the use of the name, coat of arms and other symbols of the municipality and to perform other activities prescribed by law and the statute.

The president of the municipality is a statutory body of the municipality who represents it and has the executive function.[52] These particularly includes: direct implementation and insurance of the implementation of the decisions and other by-laws of the municipal assembly; proposing of regulations and other by-laws to be adopted by the assembly as well as the procedures for the decisions of the municipal assembly regarding the issues within its scope of competence; ensuring the implementation of delegated responsibilities within the rights and responsibilities of the Republic and/or forms of Territorial Autonomy; providing guidelines for and co-ordinate the activities of the municipal administration; proposing the appointment and removal of the head of municipal administration and/or the heads of administrations in charge of specific fields; ordering the execution of the budget; passing specific by-laws according to the authority vested in him/her by law, the statute or decision of the assembly and performing other activities in accordance with the statute and other by-laws of the municipality. As it is seen, the president of the municipality has the political and material responsibilities for the municipality.[53]

The municipal council, with up to 11 members, is the body which coordinates the functions of the president of municipality and the chairman of municipal as-

52 See, for example, art. 6 par. 2 and art. 51 Statute of the City of Nis, June 6, 2002.

53 More on the president of the municipality function in art. 40 and 42 of the Law on local self-government.

sembly and control/supervise the work of the municipal administration.[54] More strictly, it executes decisions and all other acts enacted by the municipal assembly. It exercises control over this regulatory enforcement and decides on issues related to the supervisory control over the municipal agencies, utility companies and services it is expressly authorized for. It may also propose the political solutions and enactment for which the municipal assembly is competent for[55], and it exercises the review over the municipal administration acts by overruling or abolishing administrative orders of the municipal administration if found not to be in accordance with the law. The municipal council, also, decides on the issue of conflict of jurisdictions between municipal administration agencies and other institutions that are entrusted with public administration powers. It is also the second instance body when the municipal agency acts as a first instance in matters that originally belong to municipalities and they are related to the rights and responsibilities of citizens, enterprises and institutions, and other organizations within the municipality's original scope of responsibilities. By the rule, this type of control does not include matters of state administration, since these do not fall within the original competence of municipalities.

The municipal administration is an integral organizational unit that deals with administrative matters on municipal level.[56] If there is a need for some sort of internal sub-divisions, this may be accomplished by organizing departments. The exception to this rule goes for municipalities with population of more than 50 000. These municipalities may have more municipal administration agencies, for example, secretariats as organizational units.[57]

---

54 It assists to the president of municipality in the performance of other activities within his/her scope of responsibilities.

55 As it is stated by the art. 44 para. 1 of the Law on local self-government "the municipal council determines the proposal of the decision on the budget of municipality".

56 The analysis of the municipal local administration shows that most of them have two or three departments. The areas for which the departments are usually organized are urbanism and residential-utility matters, economy and financing, and general public administration matters and social services. In some cases, municipal administration includes four or even five departments (when general public administration issues are separated from social services).

57 Art. 49 of the Law on local self-government. But, in the case the municipal administration is a single unit, it will be managed by the head of the municipal public administration. However, if the municipal administration is organized to consist of several administrations, such administrations shall be managed by the heads of administrations. Further more, the internal organizational units may be established within the administration to perform supplementary activities, headed by the heads of organizational units within administrations (appointed by the head of administration). The head of municipal administration is requested to report in respect of his/her activities and the administration activities to the municipal assembly and the president of municipality, in accordance with the statute of municipality, and the decision of the municipal assembly regarding the municipal administration.

The primarily task of the municipal administration is enforcing regulations of the municipal assembly, the president of municipality and the municipal council.[58] In addition, it can prepare drafts of regulations and other by-laws ton request by the municipal assembly and the president of municipality and to provide expert and other activities to the same bodies. On the other hand, the municipal administration enforces the laws and other regulations of the Republic of Serbia, whose enforcement has been delegated to municipality.

As a difference to the previous Law on local self-government, present Law has introduced two new institutions: the main architect[59] and the municipal manager[60]. Both of these officials, within the context of the municipal administration, are not mandatory and it is up to the president of the municipality if they will be appointed at all.[61] Additionally, president of the municipality can remove any of the appointed officials without prior consent from the bodies of the local self-government unit.

Through out the Serbia only the City of Belgrade has its city architect and city manager who were appointed by the city mayor.[62] Elsewhere in Serbia it is not the case, not just because the local bodies have not been inaugurated, but primarily because there is no experience at all with such institutions.

According the Law, the main architect has power to:

- launch initiatives for the preparation of a municipality planning layout, as well as for the amendments and addenda to the municipality planning layout;
- provide guidelines for the development of architectural designs for the purpose of protecting the architectural values and preserving the environmental values of the municipality's particular parts and facilities;
- cooperate with the institutions for the protection of immovable cultural values and the protection of special natural values;

58 According to the art. 48 of the Law on local self-government, municipal administration conducts the administrative control over the enforcement of the regulations and other general by-laws of the municipal assembly and it can resolve, through the first-instance administrative proceedings, the issues related to the rights and responsibilities of citizens, enterprises, institutions, and other organizations within the municipality's original scope of responsibilities.

59 Art. 54 of the Law on local self-government.

60 Art. 55 of the Law on local self-government.

61 In addition, and in accordance with the law (art. 54 para. 7), other main experts in specific fields may be appointed within the municipal administration (primary health care, environmental protection, agriculture, etc.).

62 More on this one is available at http://www.beograd.org.yu/cms/view.php?id=516839.

- give opinion on the architectural projects of major significance to the municipality, and perform other activities specified in the by-law on organization of the municipal administration.[63]

The second official, according to the statute of municipality, responsible for the purpose of performing municipal activities is the municipal manager. President of the municipality, on behalf of the municipality, and the municipal manager have to sign the contract aimed to regulate their mutual rights and duties (i.e. to determine the conditions and the manner in which the services of the municipal manager will be used). The manager function is defined to stimulate economic development, entrepreneur initiatives, private-public arrangements and partnerships, co-ordinate capital investments and activities for attracting capital by proposing projects and adjustments of the regulations with impeding effects on business initiatives. All these activities are aimed to meet the needs of citizens and have to ensure environmental protection as well.[64]

4.3. Relations between the republic administration and the local self-government units

The relationship between the central and local levels stands to be base and an indicator of the extent of democratization and modernization of a country's public administration. The Law on Local self-government of 2002 has changed the relationship between Republic and local self-government bodies substantial self-government in Serbia.[65]

63 Presently, in Serbia discussion is going on because of illegal construction. In past couple of decades, so many buildings and other construction forms have been built, that main architect will have tough job to make. Close co-operation in this meter with the Republic bodies will be needed as well.

64 Art. 56 of the Law on local self-government. Basic information on appointment of the city manager in Belgrade and his responsibilities are available on the following page: http://www.beograd.org.yu/cms/view.php?id=516823.

65 Previous Law on local self-government from 1999 established extensive state authority over the local self-government. It should be noted that relationship between the mentioned two levels was essentially determined by the political structures in power on both sides!? In the case of different political parties in power on state and local level, obstruction instead of constructive co-operation between these two was primarily seen. Such temporary disappearance of local self-government has initiated ideas and particular steps, after political changes in 2000, in developing creative and useful relationships in the process of pursuing the welfare of the country and its population.

Competences of the Serbian local self-government are defined by the *numerous clauses* principle.[66] The core of this system is that local self-government is competent for powers which are explicitly stipulated by the normative acts. Further more, the law assumes that all rights and authorities belong originally to the state, which can delegate them when appropriate and on a case by case basis. A local self-government unit should not assume that it has a right unless explicitly provided by law and in addition a detailed list of activities determines which may be performed by municipalities and cities and which by other authorities.[67]

But, as mentioned earlier, article 105 of the Law on local self-government provides a legal ground for mutual cooperation between the bodies of the Republic, Territorial Autonomy and of the local self-government units with each other in accordance with the Constitution, law, and other regulations.

Local self-government bodies may initiate the procedure before the central bodies[68] for regulating the relations of significance to the local self-government and undertaking measures relevant for resolving the issues within the framework of rights and obligations of the local self-government unit as well as submitting written recommendations and proposals regarding the actions of the central bodies.[69] Also, the local self-government bodies may put forward the request regarding the interpretation of the legislative acts of a vital interest for a local community and the enforcement thereof. The last one, based on available data is rather a symbolic, and deals with the participation in the

66 Comparative approach to this question shows existence of another type of relationships between the mentioned two, which is based on the general clause. The core of this system is that constitutions and laws proclaim only the general areas and directions of the local self-government activity. According to the general clause, the local self-government possesses all functions that are not excluded expressly by law i.e. local self-government encompasses all functions that are not prohibited explicitly or are not entrusted to central and other authorities.

67 From this perspective, Serbia`s model, for central-local administration relationships, is not in accordance with the European Charter of Local Self-government. Art. 4 of the Convention states "local authorities shall, within the limits of the law, have full discretion to exercise their initiative with regard to any matter which is not excluded from their competence nor assigned to any other authority."

68 Territorial Autonomy bodies included when necessary.

69 Art. 106 of the Law on local self-government.

preparation of laws and other regulations relevant to the implementation and development of the local self-government.[70]

Concerning the reverse direction of the co-operation, the bodies of the Republic and Territorial Autonomy have power to:

- inform the bodies and services of the local self-government unit, on their own initiative or upon the request of the bodies and services of the local self-government unit, of the measures taken or intended to be taken in the course of the implementation of laws and other regulations; protection of constitutionality and legality; the acts by which they are violated, and the measures for the elimination of such acts; citizens' right to local self-government; other issues of direct interest to the implementation of the local self-government system and work of the bodies of the local self-government unit;
- provide professional assistance to the bodies and the services of the local self- government units in relation to the performance of their duties, particularly in establishing the information system and in the computerization of work performed by the bodies and services of the local self- government units;
- file requests for reports, data and information on the activities performed within the rights and responsibilities of the local self-government unit, and matters of interest to the role and functioning of the bodies of the Republic and Territorial Autonomy in the field of local self-government and
- perform other tasks in accordance with the law and other regulations.[71]

According to the law[72], any local self-government unit has the right (and in the same time duty) to perform efficiently and adequately its original and delegated responsibilities without the interference of the central authorities.[73]

---

70 This power of the local self-government units corresponds with the ministries duty to cooperate with them and their associations when preparing legislative acts which are important for their development. It has to be noted that ministries autonomously will decide whether a certain law involves local self-government issues or not. If the ministry decides (on a discrete base) that an act is not of importance for the local self-government, local community bodies will be not included in drafting of the act. In past, ministries have decided to co-operate with local self-governments in just few cases and, with this way of acting, have breached the art. 4 para. 6 of the European Charter of Local Self-Government.

71 Art. 107 of the Law on local self-government.

72 In particular, articles 8 – 10 of the Law on local self-government.

73 Art. 4 para. 2 of the Law on local self-government states that "the local self-government unit may be restricted in performing its original responsibilities only under circumstances and conditions determined by law and in accordance with the Constitution."

Also, local self-government unit is free to select priorities by itself. However, any local self-government has financial restrictions in respect to the size of the budget that is to be spent to satisfy the local needs. So, according to the law, every local self-government has a limited budget, i.e. the central authorities determine for each of the local self-government how much money will be spent in a fiscal year for local needs, taking into consideration the level of development, the population of the unit, etc. If local self-government provides more money from its sources, then the "surplus" must be transferred to Republic funds, or additionally can be approved by the central authorities to be used by local authorities.

Local self-governments have the right to improve the conditions in some social fields which are presently in the charge of the central authorities. In the field of education, for example, they can give some extra money to kindergartens, primary and secondary schools (originally administered and financed by the ministry of education) in order to provide teaching aids, organize transport for pupils from remote villages, reconstruct school buildings and do everything else that is not covered by the annual budget of the ministry of education. The same opportunity exists in the field of health care, (where the local self-government can invest in medical equipment and medicines), sport and culture (where they can give extra money to libraries, sports associations, etc).

Based on this knowledge, it is interesting to mention that central (disitrict) level officials who are legally responsible for certain public services are not held accountable by citizens at the local level, while local officials, who lack the authority and resources to address the problem, are held directly accountable to the public. This paradox illustrates that the inherent basic accountability that exists at the local level is fundamentally more vibrant today than at higher levels of government. In addition, as a generic guiding principal of modern public administration, service provision should occur at that level which provides the optimum balance between efficiency and democratic accountability.

Another common point between the central and local self-government is central bodies control over the local self-government bodies. According to the Constitution, the state may intervene with the work of municipality only in the manner stipulated by law.

On the other hand, ministries have administrative authority which enables them to control and guide the conduct of business of the local self-government units. A competent ministry is entitled to the reports, information and data regarding the work of local agencies when exercising both original and delegated powers. If there is any malfunction, ministries will inform local self-government bodies about it and undertake all necessary measure in order to

redress the problem. These measures may vary which highly depends on the kind of a malfunction.

Ministry for state administration and local self-government[74] (competent body of the Territorial Autonomy)[75] has a special role in dealing with these issues. It has supervisory authority over the individual and general acts brought by the local self-government bodies.

The competent ministry is authorized to control the implementation of a regulation or other general by-law enacted by the local self-government dealing with the freedoms, rights and duties of a man and citizen. If such acts can cause "unrecoverable damage, deny or restrict guaranteed freedoms or individual and collective rights, or severely violate common interests", the Government may impose provisional measures within the 15 days from the day when proposal of the competent ministry was made. Suspension of the implementation of such act lasts until a decision is made by the Constitutional Court.[76] In the very same manner the competent ministry/competent body will react if the statue or by-law does not comply with the Constitution, the law or another Republic regulation (statute of the Territorial Autonomy).

The situation is slightly different if the competent ministry considers an individual act of a local body to be inconsistent with the local self-government statute. In that case the ministry will point at this inconsistency to the assembly of a local self-government unit so that it can undertake necessary measures in that respect. If a local assembly does not act upon it, the ministry will initiate the procedure before the Supreme Court of Serbia and simultaneously put forward a proposition to the Government to suspend the act in question.[77]

If a by-law enacted by a body or service of the local self-government unit has been found non-compliant with the law or any other regulation and/or any decision or other general by-law enacted by the local self-government unit, whereas no protection against such a non-complying by-law has been provided by administrative action, the competent ministry/competent body shall propose to the assembly of the local self-government unit to repeal or annul such a by-law. In cases when there is an allegedly illegal act which cannot give rise to the judicial review, the competent ministry will put forward a proposition to the assembly of a local unit to annul or abrogate such an act. If the as-

74 Hereinafter "competent ministry".

75 Hereinafter "competent body".

76 According the art. 108 of the Law on local self-government, the proceedings before the Constitutional Court for the purpose of assessment of the constitutionality and legality of the disputed general by-law have to be initiated no later than 15 days from the suspension of such regulation.

77 Art. 111 of the Law on local self-government.

sembly does not proceed upon this proposition within a month, the competent ministry will either annul or abrogate this act.

The Government of the Republic has special authorities over the units of the local self-government. This authority can be activated in cases of provisional measures that are necessary to restore the dysfunction in the conduct of business of local self-government. If the assembly of a local self-government unit does not perform its tasks for more than three months[78], or it performs them in an inappropriate way which infringes Constitutional and legal rights of citizens, or it heavily distorts public interest, the Government will notify the assembly of a local self-government unit and demand the appropriate steps to be taken within a certain time limit. If the assembly fails to act accordingly, the Government will dissolve that assembly and form a temporary body of the local self-government unit consisting of five members. This body appointed by the Government will be in charge of all tasks and duties that originally belong to the municipal assembly and its council. In that case, the president of the Parliament of the Republic will organize new elections for new members of the assembly within a year after the assembly dissolution. However, if the current delegates in the assembly of the local self-government unit have no more than six months left to the end of their term, new elections will not be organized.

There are also some powers of a local self-government assembly as safeguards of its rights. The assembly of a local self-government has power to initiate the procedure before the Constitutional Court for judicial review of the legislative and other acts of the Republic that directly infringe the rights of local self-government explicitly guaranteed by the Constitution (the original competences of the local self-government enumerated in the art. 113 of the Constitution).[79]

Apart from the mentioned relationships that may occur between the central and local administration, there is also the one that is established when local agencies perform delegated administrative matters.

78 Or if the local self-government bodies are not established within the 2 months after the local elections, Government of the Republic will form a municipal council. It is interesting to add that the last local elections in Serbia "are not over yet, inspite the fact they were held back in September this year". Namely, most of the local self-government units still do not have their local self-government bodies.

79 On the other hand, if a local self-government body holds that such an infringement was caused by an individual act of a body of the Republic, it can bring a lawsuit for the protection of local self-government before the Supreme Court within 30 days. The Supreme Court may either dismiss the case, or grant a relief that results in the annulment of the act which is the subject matter of the case, or put a restraint on its further enforcement. In this type of cases the Court applies the Law on Judicial Review of Administrative Matters.

Ministries have a general authorization to exercise administrative control over all delegated matters and authorizations.[80] The ministries whose affairs have been delegated "exercise a direct control over the legality of the conduct of business and they are authorized to issue mandatory instructions thereof, and if it is necessary, they can take over the performance of these tasks or ensure a proper enforcement in some other way." This type of the control is conducted through districts.

If a ministry decides to take over delegated matters, it will also deny the appropriations related to the delegated matters. If a local agency does not follow the eligibility conditions for its employees or does not enact the ordered enactment, the issue of the responsibility of the administration officer who is in charge of this agency may arise.

In cases of natural disasters and some other emergencies, if a local self-government does not undertake necessary measures timely to prevent a prospective damage, competent body of the Republic will step in to take on these measures. Expenses relating to these measures will be always covered by the budget of the local self-government unit. The body of the Republic that acted upon this matter will also initiate the proceeding for the determination of the responsibility of the local self-government body that failed to provide necessary measures.

5. How Serbian public administration should be reformed

Serbian public administration reform should be aimed to secure, in a broader sense, economic stability and quality of living standard and, strictly, high quality of services offered to the customers (citizens and business). Both of these

80 The Law on State Administration regulates the position of ministries with respect to the agencies of Territorial Autonomy and local self-government, when performing delegated administrative matters. With respect to agencies and organizations to which state administration matters have been delegated, ministries are authorized to: request reports, information and data, issue mandatory instructions, notify on the nonperformance of the delegated matters and set up a time limit of no more than 30 days for their performance, take over the performance of a particular administrative matter if a competent agency does not act upon it after the notification, take over the performance of certain administrative matters that have not been accomplished by a local agency, for a period determined by the decision of the ministry, provisionally transfer a ministry employee to the agency performing delegated matters, prescribe the eligibility conditions for the employees in an agency entrusted with delegated administrative matters and determine a number of the employees thereof, prescribe the manner in which the official records on delegated matters are to be conducted, annul or abrogate the acts of agencies brought in the course of delegated matters, save for the acts which are the results of the administrative procedure, order an enactment within the local agency competence and this order is safeguarded by the ministries' authority to act accordingly if a local agency fails to follow the order.

aims will have enormous impact on quality and efficiency of economical and social reforms in general.[81]

Unfortunately, instead of having new constitution just after 2000, Serbian Government starting point for the reform will be, most probably, provided by the Constitution from 1990.[82] However, this does not impose any limitations in defining the strategy compatible to future changes of the present constitution. All relevant political subjects` commitment to the principles of the democratic state such as rule of law, citizen's suverenity, transparency, accountability, dividing of powers, decentralization of power, representative democracy, cheeks and balances, minority protection, human rights will make the whole process much easier.[83]

Public administration reform should take into account historic development of the country as well as its essentials, but in the same time, if it is aimed to be successful, it must comply with the European and world trends in society development.[84] The most important trends in modern society development which impact on public administration structure and public sector in general are:

- Transition from industrial to information(al) society,

81 As it is known, reform of public administration as an expensive process requiring studious approach and aggregation of efforts of all the stakeholders (political actors as well as civil servants). Starting point should be enacting of the Public Administration Strategy reform in Republic of Serbia containing evaluation of present situation, reform principles, key areas of reform and frameworks of the needed reforms in other areas of which such reform depends on (i.e. fiscal decentralization, mechanisms of public administration control, introducing modern ICT etc.). Parallel to the mentioned reform based on the common principles of the European Administrative Space (especially "good governance" and "open government" concepts), several programs of national importance should be conducted in particularly: the poverty Reduction Strategy together with the Strategy of Information Society Promotion.

82 In addition, present conditions and very late start of the reform (in comparation to other transitional countries) make this aim even harder to achieve. Inspite the statements made from some officials "that beside all disadvantages, Serbia will be in a position to use others experiences aimed to avoid already known mistakes", my opinion is, that lack of time can put additional pressure on those responsible to plan and implement reforms. It is important to understand that mechanical reception of any relevant (foreign) experience, with no taking into account Serbian society specifications, can waste (precious) resources and time. It is equally important that public administration reform means reform of state itself on one side, by changing its organization and functioning, and, maybe even more important, changes in the way of how citizens and those who personalize institutions are approaching to the state on the other side.

83 The real question in Serbia nowdays is "If all political parties respect all the mentioned principles and if so to which extent!?"

84 It should be mentioned that we are talking about the constant process over which can testify facts, not just in transitional countries, but in most developed countries as well. Look for examples of Norwegian ministry of modernization (http://odin.dep.no/mod/engelsk) and ministry of local government and regional development (http://www.odin.no/krd/engelsk).

- Transition from national to global economy,
- Transition from short-time to long-time planning,
- Transition from centralism to decentralization[85].

5.1. Basic aims and principles of the reform

Basic aims of the reform are: building the democratic state based on a rule of law, as well creating citizens oriented, accountable, transparent and efficient administration.

For achieving all these, Serbian Government should follow basic principles, such as:

- *Decentralization*. One of the elementary presumptions for general democratization of the society is dividing the powers between the central and local levels. Citizens participation in public policy creating process is much more important in the cases which are known to them. Decentralized power is in position to be much better informed on the needs and requests from the individuals, which can produce better quality of the fulfilling the public needs and general development of the local community. The other side of this example creates greater responsibility for decision makers and reduces the possibility of mis-using the powers. Decentralization can be achieved through the application of one of the three (known) models (or even of their combining):
- Devolution model is the fullest model of decentralization due to fact that it means the transfer of the state powers biggest share to the exclusive jurisdiction of the local self-government. In this way, local self-government can, in specified areas, in compliance with the positive laws, act independently which is followed by the financial independence from the central government as well. Local bodies are entirely responsible for the decision making process and their implementation, and in the case of dispute between the local authorities or local on one side and central on the other, only the responsible courts can intervene, if the law or Constitution were breached.
- Deconcentration of the powers goes for decentralization of the central administration organs (especially when ministries and special organizations are in question) in a manner that they will create their branches aimed to perform their tasks in more economic and efficient manner combined

85 Serbian Government should accept decentralisation concept on the basis of which a new distribution of competencies between the state, districts and municipalities based on a change in perception of the public sector role within the society and searching for the optimal level of its regulation from the public interest point of view.

with easier delivering of services to the citizens. This model is really not a model of decentralization due to fact that local self-government bodies do not have any impact at all on the work of central bodies.

- Delegation of the power stands to be a compromise solution between the first two. In this case local self-government is, instead of the central one, directly responsible for some public functions with the control kept by the central government. It is followed by the obligation on the central government side to provide sufficient (financial) resources for local units concerning their responsibilities.
- *Professionalization.* This process means creating well trained, responsible and efficient administration. Achieving only depolitization of public administration and not the mentioned goals would not be seen as reform of public administration at all. Because of that, these two principles are closely related to each other and they are very important for the reform. If pledging that professionalization should be successful it is important to provide: objective choosing of the employees based on knowledge and experience, permanent education of servants, objective monitoring and marking over the servants, introducing the motivation and rewarding mechanisms (promotion based on achieved results is included), simulative wage-scale system, introducing clear rules for behavior and treating of responsibilities, fighting against all forms of corruption with introducing clear mechanisms of work and responsibilities control. Depolitization means clear differentiation between the two processes i.e. process of political creating of the decisions at one side and process of their legal norming and exercising in accordance with the present rules. Application of this principle in all the transitional countries is of essential importance for the transformation of public administration in the citizen-oriented governance. It may take two forms: developing and strengthen of carrier system (guaranties for the promotion based on professional achievements included). This, before all, means clear defining working places which are available for the professional politicians at one side and top-position within the public administration available to the professionals on the other. This, also, means and undoughtable division of work process and responsibilities between these two categories - politicians and top-managers in public administration. Introducing mechanisms for preventing the political influence on carrier service employees. Depolitization is seen to be a presumption in creating permanent and stable public administration, which will then create the conditions for introducing professionalism and continuity on a strategic level of decision making. All this can be achieved with defining the civil servants legal status as well as

building the concepts of public administration role and importance for the development of the society in general independently of political parties.

- *Rationalization*. Rationalization within the context of public administration is aimed to create its optimal organization which will be in a position to provide services in an efficient manner and of satisfying level with engagement of minimum required personal aimed to decrease expenditures. This whole process is consisting of few elements: on the macro organizational plan (the whole public administration organization) it means clear dividing and distribution of competences and responsibilities between the different levels of the authorities and between the different organs at the same level of powers. This is based on a very precise legal framework and protecting vertical and horizontal coordination of the work; on the micro organizational plan (within the organs and institutions) it includes clear dividing and distribution of competences and responsibilities between the different parts inside of the same organ, application of the modern work methods and providing services, enabling lover levels for the decision making, introducing efficient horizontal coordination and control as well as real judgment of the needed personal for each of the tasks (it includes functional analysis of the obligations of each of organs), application of work modernization principle and careful planning for the servants which will lose their jobs and
- *Modernization*[86].

5.2. Introducing ICT in Serbian public administration as a form of its modernization

ICT[87], influencing all the segments of the life, became focal point for the governments worldwide for the concept of the of making public sector information available to the citizens and business. Modernization as a part of the overall public administration reform is defined and coordinated to be its most efficient part.

86 Modernization primarily means introducing technical and technological equipment in the public administration (i.e. modern ICT). A trend of transformation of industrial to information society will request huge resources for creating databases, Intranet system between the state (and local) administration with introducing e-business and e-sign into daily activities of administration.

87 Having the grate potential for information and data collect, maintain and transfer in accurate an efficient manner, ICT are bringing one of the positive effects to the public administration quality reform. Furthermore, ICT (combined with some other measures) can eliminate bureaucracy and provide greater transparency as well as support establishing of the Information Society which brings, in return, a new quality in the society development based on ICT application.

Modernization principle means, at the first place, application of modern ICT in the public administration (i.e. introducing technical and technological equipment), which is fully in compliance with the public administration transformation process from Industrial Age to the Information Age.

The goal of public administration modernization is that with introducing ICT in the work of organs at the central and local level provide to citizens possibility of influencing on the public life (i.e. incorporating citizens into the civil sector and public life and creating the public policy through the direct interaction). ICT are bringing to the citizens electronic accessibility to variety of services based on transparency as well as to provide a feedback for the public administration functioning and conducting of public business. All this makes Internet application more fruitfull in creating public services more oriented towards citizens. Process of society democratizations is impossible and due to this one there is a strong need of balancing and harmonizing of these two sides.

Modernization is seen to be as the first element in the rationalization process. Providing the services becomes more efficient and reliable, makes access to the information more convenient to the citizens (as well as conducting the business with the public administration) which will create the conditions of cutting the number of the officers in the future. From this perspective, modernization process, inspite of being a great investment for establishing the system and its functioning, at one side, provide a framework for introducing services offered to the citizens, at the other is multifunctional.

Because the whole process is very complex, it has been developed in the phases with phases and coordination. There are three main phases of Republic of Serbia public administration modernization:

- *Current Status* as the first phase includes: Evaluation of the present informational system[88], conduct analysis of how the present legal framework

88 Common informational system of the Government of Republic of Serbia is yet to be defined by the National Strategy of Information Society as well as with the National Strategy of Informatization of Public Administration. Both of these are in competence of the Agency for informatics development and Internet (formerly Agency for Internet and Informatics). The Agency was established by the Law on Ministries (2004) to provide specialized services related to development and functioning of information system of state administration and local governments, use of Internet in state administration, data protection etc. Furthermore, Informational systems of the central administration and local level has to be found on the common Government Informational System where the exchange of information will be defined as a standard (this will improve integration and high interoperability based on highly developed (horizontal) cooperation between the local informational system at one side and (vertical) with the republic organs at the other). For the same purpose, it is needed to deregulate and simplify the working procedures, where possible, aimed to reform such processes based on ICT standards.

influence fulfilling defined aims and to what extent is needed their change for supporting the ICT application as well as preparation and enacting the acts purposed to legal verification to the electronic documents, exchange of data, submitting the request in electronic form etc.

- *Integration and implementation* as the second phase includes: Projecting and building up of independent communication infrastructure of the central administration (as well as the infrastructure of the local administration) taking into accounts all the present resources and (preferably) compliance with the international standards, defining of standards for vertical and horizontal communication by the ICT, providing the access to present systems as well as exchange of data and information, reform of the working processes as well as their simplifying at central and local levels in accordance with ICT and training and motivation of the personal.
- *E-services to the customers* as the third phase includes: Providing the citizens and business variety of public services offered by the central and local level administration such as documents testifying over the personal status of the citizens, permissions, tax forms and opportunity of participation in Internet forums.

Creating a more efficient public service[89] in Serbia, oriented towards citizens and based on ICT, has officially started together with preparation work on e-government.[90] It is presumed that the e-government in Serbia will improve the quality of the citizens lifes in many ways and accumulate grate savings in long term and economic aspect.[91] For achieving mentioned, it is not enough to publish information at Internet and to offer variety of services to the citizens, but to restructure the public administraion on a vertical and horizontal base (to establish communication between all te sectors in the public administration as

89 At the first place this stands for cheaper and faster providing of (public) services.

90 Until 2000 Serbian Public Administration had been on the extremely low level when it is about ICT usage in delivering public services. Often even ministers themselves did not use computers and just a few ministries had websites! Since October 2001 when the Serbian Government signed an agreement on cooperation with IBM Company and introduced licensed software in state institutions, started the campaign of introducing (modern) ICT in the Serbian public administration. Formally, first steps in coordination and promotion of e-government were made by the Council for public administration established as a specialized consultative body of the Government on February 28th, 2001.

91 Not so positive experiences (rather called failures) in different communities can provide a precious knowledge for avoiding future mistakes in Serbian case. Such practice, for example, took place in Finland during the early stage of e-government introducing when the Finish State failed to persuade its population to buy electronic identity cards to simplify access to public services.

well as local administration aimed to achieve much higher level of operativity and efficiency). A confirmation seen worldwide is that e-government is directly related with the organizational changes within the public sector as well as with the reforms at the state level.

Generally speaking the Serbian Public administration personal is not familiar with ICT. Exceptions do exist in cases, particularly when we are talking of younger administrative officers. Other employees, mostly older officers, do not posses sufficient knowledge of ICT.[92] It is so, due to the several reasons: lack of enough tools necessary for staffs` work (as well as the supportive work environment) i. e. the lack of modern computers and information nets within the Public administration[93], maintenance of bureaucratic approach in Public administration especially among the middle-aged and more senior administrators (particularly seen in the form of the fear of using computers and resistance to any changes)[94], insufficient motivation for learning how to use ICT (lack of clear satisfaction for themselves after applying the ICT within their workplace, low salaries as well as the lack of the understanding of the contribution they make to the quality of Serbian citizens life with such an effort).[95]

The measures which could overcome this situation are: ensuring the training of administrative personal in a rather similar way after which they will be in a position to share the understanding and build the necessary environment to apply (new) learned skills. Continuous training seasons are aimed to secure the implementation of new acts according to the specialization obtained during the trainings and to know how to deal with the revolution in, between

92 This does not stand for each singular case, but according to recent surveys it may be seen as a rule. Compare, findings of the research conducted through the project: "The modernization of Public Administration in the City of Nis", Faculty of Law in Nis under the TEMPUS Programme in 2001.

93 There is a gap between the needs and possibilities. Naimely, it is not realistic to argue about efficiency achieved through a variety of computer-based tools and solutions on a daily basis when resources are rare. It should be mentioned that up-to-date technologu can be provided with the help of foreign donors.

94 In the same light should be seen unsatisfactory knowledge of languages by the public administration staff. That resulted in lack of enthusiasm for taking to foreign experts: it was considered a loss rather then a benefit.

95 Serbian public administration staff is getting old, and there is an obligation of ensuring continuity of professional and leadership capacity. Therefore creating (and preserving) climate for encouraging (already) qualified personal to remain within the public administration rather than seek opportunities in the private sector together with learning how to use ICT as well as foreign language(s) is seen to be one of the goals of great importance for the whole public administration. There were situations earlier that the funds allocated subsequently for training courses in ICT in central state administration from the state budget meant the training of hundreds, if not thousands of state administration employees, a considerable quota of which then left state administration for the private sector.

the others, documentary service, accountancy and staff records which necessitated the of further thousands of employees of different levels. This new approach to public service training and education focuses on outcomes rather than inputs, with particular reference to the competencies required at different levels to build individual and organizational capacity. Good quality training for high-ranking state and local government leaders and officials must be based on concurrent (or even preceding) scientific work. The trainings should be conducted with the foreign and domestic trainers (experts equip with the sufficiently knowledge of environment, law and government, traditions and culture).

6. Conclusion

Summarizing the past and present developments of Serbian public administration it should be underlined that its competences and organization have been adjusted to the complex state forms in which the Republic of Serbia participated in.

During the time, Serbian public administration competences were transferred to the "heavy competent" local self-government or to the relatively weak (con)federal state administration. Its organizational element has followed the actual trend of competence transferring.

Currently, the Republic of Serbia has heavily centralized systems inspite the fact that there is one Autonomous Province.

In addition there are districts as de-concentrated bodies of the Republic administration.

Relatively weak local self-government in the Republic of Serbia has been conducted through municipalities, cities and the city of Belgrade.

Concerning the Serbian public administration reform we may conclude that it is going very slow. Inspite of fact that the mayor stakeholders such as Serbian Government, Parliament, Ministry for Public administration and some corresponding agencies, have been identified, it has been done little (or nothing) to avoid overlapping of their competences and responsibilities and strategic-coordination. Since the democratic changes in 2000 "the reform approach" was not good enough, lacking clear strategy and missing to set proper legal framework for reform due to which some of the laws are missing for too much time (i.e. the Law on Public administration and Law on Civil Servants).

Education and training of civil servants, performed with decisive support of international organizations and donors, is in compliance with broad social aim of achieving the public administration fit and capable to change and to adjust to new circumstances. Some activity is going on in the sphere of e-go-

vernment parallel to already started decentralization process. But due to some political disagreement as well as the existence of the Constitution supportive to centralization there are some delays. At the end, there is an impression that the transformation of the public administration is heavily influenced by the ambitious attitude towards European integrations.

Documentation

1. European Charter of Local Self-Government from 1985.
2. Ustav Republike Srbije (Constitution of the Republic of Serbia), Official Gazette of the Republic of Serbia, No. 1/90.
3. Zakon o Vladi Republike Srbije (Law on the Government of Serbia), Official Gazette of the Republic of Serbia, Nos. 5/91 and 45/93. Predlog zakona o Vladi RS (Draft of the Law on the Government of the Republic of Serbia).
4. Zakon o teritorijalnoj organizaciji i lokalnoj samoupravi (Law on territorial organization and local self-government), Official Gazette of the Republic of Serbia, No. 37/91.
5. Zakon o radnim odnosima u organima uprave (Law on the Employment Relationship in the State Administration), Official Gazette of the Republic of Serbia, Nos. 48/91 and 39/02.
6. Zakon o drzavnoj upravi (Law on the State Administration), Official Gazette of the Republic of Serbia, Nos. 20/92 and 48/93.
7. Zakon o nacelima organizacije drzavne uprave (Law on the principles of organization of the State Administration), Official Gazette of the Republic of Serbia, No. 56/93.
8. Zakon o utvrdjivanju odredjenih nadleznosti Autonomne Pokrajne (Law on determing certain competences of the Autonomous Provinces), Official Gazette of the Republic of Serbia, No. 6/02.
9. Zakon o lokalnoj samoupravi (Law on local self-government), Official Gazette of the Republic of Serbia, Nos 9/02, 19/04 and 33/04.
10. Zakon o ministarstvima (Law on the Ministries), Official Gazette of the Republic of Serbia, Nos. 19/04 and 84/04.

11. Uredba Vlade Republike Srbije o nacinu vrsenja poslova ministarstava i specijalnih organizacija u mestima razlicitim od mesta njihovog sedista (Executive order on the conduct of affairs of ministries and special organizations in places other than their place of seat), Official Gazette of the Republic of Serbia, Nos. 3/92, 36/92 and 52/92.

12. Odluka o delegiranju postupanja u upravnim stvarima upravi Autonomne Pokrajne Vojvodina (Decision on delegating the performance of public administration matters to the administration of the Autonomous Province of Vojvodina), Official Gazette of the Republic of Serbia, No. 5/92.

8 ELECTRONIC DISCOVERY: THE MANAGEMENT AND IT APPLICATION[1]

Yue Liu

1. Introduction

As modern society becomes more technically advanced, complex litigation was sure to follow suit. Over the last twenty years, a new phenomenon has surfaced in civil litigation. It is no longer sufficient for a party requesting discovery to seek paper alone. It is also no longer sufficient for party responding to discovery to review paper files alone in an attempt to satisfy the discovery request. In the Microsoft antitrust litigation,[2] countless employment related actions,[3] and even in routine divorce cases;[4] the evidence takes a new form. E-mails, chat room transcripts, databases, spreadsheets, web browser history files, and information derived from system backup tapes are replacing conventional paper documents. Just as computer has become an indispensable part of modern business, discovery of computer-generated electronic information has become an indispensable part of modern litigation.

However, despite the growing importance of the information stored in the digital format, computer based files are often overlooked subjects of discovery and sources of helpful information in litigation. There is widespread perception that the management of electronic records in most organizations is woefully inadequate, and that gives raise to many of the problems associated with electronic discovery. The research indicates that few organizations manage their electronic information with the same attention that they formerly paid

1 This paper is based on my previous master thesis for the L.L.M., in Stockholm University. I hereby owe my great thanks to my supervisor Professor Jon Bing, who has provided me a lot of seasoned guidance during my research. As well as Professor Cecilia Magnusson Sjoberg who supported me and encouraged me to do my research here in Oslo. Thanks also go to Ms. Pia Laakso, Mr. Tobias Mahler and Ms Anne Grunn B. Bekken, who had helped me for other practicalities. Last but not least, it would also be difficult to finalize this paper without Mr Georg Phililp Krog's suggestions on the revisions.

2 See, United States v. Microsoft Corp., Civil action 98-1232(TPJ) (D.C.D.C.12 November 1999) (Findings of facts).

3 See, Samuel A. Thumma, Electronic Mail in the Workplace: Litigation Trends for 1998 (visited April 22,2003) http://www.brownbain.com .

4 See, Maria Gold, He-said, She-said Divorces Take on Twist With E-mail, Boston GLOBE, 2 May 1999,at A 16.

to their paper documents,[5] compounding the problems of volume and scope when the electronic records become subject to discovery.

The discovery process has a significant impact on the results of numerous cases.[6] In many cases, electronic discovery procedures can be extraordinary.[7] Many of the reported cases on electronic discovery, failures of the attorneys to understand their own client's computer systems, routines, capabilities, and limitations were at the heart of the problem.[8] Early identification of potential discovery problems and early resolution of these matters may be the key to reducing costs and delay in cases involving electronic discovery.

Needless to say, this reality has attracted widespread attention among lawyers and the public at large. However hot debate surrounding this topic seems to focus more on the legal skills being used during the litigation process, rather than taking the management of electronic discovery before and during the litigation as a whole. Moreover, although the concern of using the IT techniques has been expressed on many levels, the importance of combining it with legal tools for effective management of electronic discovery has not aroused enough attention.

Talking about the electronic discovery, it is unavoidable to come across the problem of jurisdiction. [9]However, I will not touch this issue here due to the length and focus of the paper. And my discussion will focus on the Federal Civil Litigation Rules of the United States, which is the law most cited in this

---

5 See, Kenneth J. Withers, Is Digital Different? Electronic Disclosure and Discovery in Civil Litigation" (visited April 25,2003) http://www.kenwithers.com/articles .

6 See Ron Chepesiuk, Trial by E-mail, STUDENT LAW, Sep.1998, at 31,31-32 (considering impact of heightened use of computer technology on legal profession, specifically litigation-related matters).

7 See, Lawrence Argon, E-mail is Not Beyond Law, PC week, 6 October 1997 at 111(the cost of reviewing ten years worth of data in a recent case was over $500,000) Kim Nash, Computer Detectives Uncover Smoking Guns, Computer World, 9 June 1997 at 1A(twelve months of e-mail generated by 50 people will cost between $60,000 and $75,000 to examine).

8 See, e.g., Linnen v. A. H. Robins Co., 1999 WL 462015 (Mass. Super. Ct.), in which the defendant was ordered to bear all fees and costs associate with computer-based discovery based on its failure," be it unintended or wilful" to respond adequately to the plaintiff's discovery requests for e-mail from back-up tapes. Id.at 8.See also GFTM, Inc. et al. v Wal-Mart Stores, Inc., 2000 WL 335558 (S.D.N.Y.), in which the defendant was sanctioned for counsel's initial representation that requested computer data did not exist, contradicted a year later by deposition testimony that the data existed when they were requested, but were subsequently destroyed.

9 Since the electronic discovery may include something published on the Internet, or produced by another party in another country, it is possible to involve the discussion of jurisdiction issues in the management of electronic discovery.

field.[10] Due to the recognition of law, electronic discovery has been widely accepted and used in the court of the US. As one of the most developed countries in the world, the US is among the earliest to recognise and use electronic discovery. Accordingly there are more case resources, and court experiences to refer to,which becomes a valuable basis of the research.

This paper aims to present some advice for managing the new format of discovery both prior to and during the litigation. Instead of basing the research on personal experience, it will learn more from the existing materials from legal journals, official documents, as well as software companies etc. The main research question of the paper is formulated as: *How can we make the management of electronic discovery more efficient?*

The research method proceeds in a stepwise manner by addressing the operational sub questions. *Section 2, From paper based to electronic discovery* will make an inventory of the difference of the electronic discovery. By analysing the advantage and disadvantage of electronic discovery, it will also explore the unique problems that need to be considered in the management of the discovery. Following on from this, the main aspect of the management through computer assistance will be laid out in *Section 3, IT assistance in the management*, which includes the security and authentication issues associated with the storage and discovery of digital information, the use of information retrieval techniques in the database, and finally the way of choosing litigation support software will be discussed. In *Section 4,Legal management tool for electronic discovery,* we will examine the relevant Federal Civil Litigation Rules concerning the duty for preserving the electronic information, as well as the sanction for the destruction along with this, some famous case decisions will be touched upon, and the retention program will be introduced. In the final section, *Section 5*, the findings of this research will be summarised and the conclusion is reported. It should be clear from my research that the efficient management of electronic discovery could be realised with the appropriate assistance of computer technology as well as the judicial tools.

2. From paper based to electronic discovery

To explore the main problems within the management of electronic discovery it is necessary to start with finding its characteristics, especially to compare with its conventional paper counterparts.

10 Electronic Discovery is formally recognized in the Federal Civil Litigation Rules of the US, while other laws has not touched upon it so literally. Therefore this rule has been most cited when talking about electronic discovery.

2.1. Advantages of the electronic discovery

Though some body of research[11] that has been developed around the topic of electronic discovery premised on that electronic discovery increases the cost and complexity of civil litigation, there is no denying that it is generally worthwhile to obtain the information required to prove a case. In fact, there are several reasons that make it desirable to request electronic over paper forms of information.

First, the cost of photocopying and transport can be reduced dramatically or eliminated altogether.[12] The time involved in reviewing and organizing evidence can be reduced by using word searching, sorting, and other forms of computer manipulation. For example, attempting to manually locate a specific information, or document or all the document that are relevant to a particular issue from a pile of files or paragraphs of the texts, can take days, while the same task can be performed in the electronic format within minutes. The cost of using a litigation support system can also be reduced if the documents are in electronic form from the start and do not need to be scanned.[13] And as the electronic discovery leads logically to electronic evidence, it stands to reason that many of the media conversion costs associated with electronic courtroom presentations can be reduced or eliminated if the documents are in electronic form from the start.

Second, electronic discovery contains information that is not apparent in its paper counterpart. Drafts of documents that were routinely lost or destroyed in the conventional paper-based world are now retrievable.[14] Evidence that would have been extremely difficult to obtain can now become traceable. For example, the electronic version may contain comments, time and data of the most recent access, updates and filenames.[15] In *Armstrong v. Executive Office of the President*, the Court of appeals for the District of Columbia Circuit ex-

11 For example see, Gregory S. Johnson, Esq, A Practitioner's Overview of Digital Discovery, Gonzaga Law Review, VOL 33:2,at 348-375; Donald C. Massey, Discovery of Electronic Data From Motor Carriers-Is Resistance Futile? Gonzaga Law Review, VOL 35:2,at 146-174;Virignia Lewellyn, Discovery the E-way, available at http://www.law.com/jsp/printerfriendly.jsp?C=LawArticle&t=PrinterF.., (last visited May 5 2003).

12 See, Mark D. Robin, Computers and the Discovery of Evidence: a New Dimension to Civil Procedure, 17 J, Marshall J. of computer and info. L.411, 419 (1999).

13 See, J. Roger Tamer, Preparing for Electronic Discovery, N.Y.L.J., 25 January 1999, at S5

14 See, Grefory S. Johnson, A Practitioner's Overview of Digital Discovery, 33 Gonz.L.R.347, 360 (1998). A more through discussion of text retrieval will come later in Section 3.2.2.

15 See, James H.A. Pooley & David M. Shaw, Finding Out What's Out There: Technical and Legal Aspects of Discovery, 4 Tex INTELL. PROP. L.J.57, 59(1995).

plained that there are often fundamental and meaningful differences in content between the paper and electronic versions of documents.[16]

2.2. Special problems of electronic discovery

Though electronic discovery has many potential advantages, it can also raise many problems for management that do not exist or are not so problematic in conventional paper-based discovery. In the following part we will give a general picture of these problems and hopefully we can put forward some suggestions by the end of this paper, which help solving these problems.

2.2.1. Preservation

Electronic documents are usually much easier to alter or damage. It is much easier to forge an electronic message than a hand written signature.[17] In the process of disclosure or discovery, paper documents maybe removed from physical files, reviewed, indexed, photocopied, and otherwise handle with common-sense procedures to ensure their evidential integrity. However, electronic information is easily changed or overwritten. Even a simple acts of opening a file, adding new data onto a hard disk, or running a routine maintenance program on a network can alter or destroy existing data, without the user's knowledge.

2.2.2. Volume

Electronic documents are voluminous; every time an electronic document is shared or exchanged a copy is created. Moreover, since a digital document is virtually invisible, and takes no discernable space, people tend to forget systematically to clean up their digital document as they used to do with their paper documents. In paper based record keeping systems, outdated records, papers with no business significance and superfluous copies are destroyed routinely, while the electronic documents were ignored and stored according to computer's order instead of people's order, offsite storage facilities, internet service providers and other third parties may also hold data subject to discovery.[18] All these add to the difficulty and cost for locating after some time.

---

16 Armstrong v. Executive Office of the President, Office of Admin, 1 F.3d 1274,1287 (D.C. Cir 1993)

17 Matthew Goldstein, Electronic Mail, Computer Message Present Knotty Issues of Discovery.N.Y.L.J.Feb.8, 1994, at 1.

18 See Michael R. Overly, Electronic Evidence in California (1999) 2-31 (a three-page checklist summarizes the preceding chapter on) Source of Electronic Evidence".

2.2.3. E-mail

Several characteristics make e-mail particularly problematic. One is the volume, which can be staggering. An estimated 108 million people are believed to be e-mail users, doubling the number of users in just four years and that number will only continue to increase throughout the twenty-first century.[19] The increase in the amount of information subject to discovery in litigation can be demonstrated by the famous Microsoft antitrust litigation.[20] The other is usually that e-mail composers fail to take much care and consideration when creating an e-mail message.[21] It can be informal, breezy and riddled with slang and jokes even in the business environments.[22] What most e-mail users do not realize, is that e-mail messages are more likely to be permanent than paper letters. These combined factors make retrieval of e-mail messages by topic difficult, even with computer based searching.

2.2.4. Deletion of document

Electronic documents are virtually impossible to eliminate entirely. The delete "key" on a computer dose little more than alter the file name and remove it from the computer list of active files. The file can be recovered using common computer utility programs or off the shelf software.[23] In the conventional paper based world, once the document has been routinely destroyed in the normal course of business, destruction is usually efficient and complete. Informal notes, drafts of documents, unsolicited mail, shopping lists are tossed into bins everyday, with little chance to recovery especially after destruction such as shredding or incineration. The discovery of deleted computer documents does not have a close analogue in conventional, paper-based discovery. Therefore

19 See Jacob P. Hart& Anna Marie Plium, Your Opponent's Electronic Media: Some "Disk-Covery" Disputes for the 21st Century, SD43 ALI-ABA 1,Jan.1999, at4; SE63 ALI-ABA, Dec.1999, at 440.

20 See supra note 1, a small software company used internal Microsoft e-mail to prove its private antitrust claims against the computer software giant. Calder, Inc. used Microsoft e-mail as evidence showing that top Microsoft executives plotted to rig Caldera's software to make the software incompatible with competing operating systems. See Leslie Helm, E-mails Show Gates, Others Plotting to Thwart OS Rivals Courts: Caldera Offers Dramatic Evidence to Back its Claims in a Private Antitrust Action Against Microsoft. L. A. Times, Apr.29, 1999, at C1.

21 See Paul F. Enzinna, An E-mail Top Teten: 5 Reasons To Worry, and 5 Ways to Sleep at Night, The Practical Litigator, July 1999,at47, 48.

22 This phenomenon was noted early in the development of computer-mediated business communication. Jolie Solomon, Workplace: As electronic Mail Loosens Inhabitants, Impetuous Senders Feel Anything Goes, Wall Street Journal, 12 October 1990,at B1.

23 Cf. further Kenneth Shear, Esq. "Delete" Doesn't Mean Delete (Revisited) Computer Forensics and Doublespeak, Electronic Evidence Discovery, 2003.

it represents a potential increase in the volume of discovery, with associates in cost and delay.

2.2.5. Backups

Most business as well as individuals periodically back up[24] their data as insurance. This is essential for recovering the important data in the event of failure. But the routine back up is designed for system-wide disaster recovery, not to be a useable archive from which individual files may be recovered. However, despite of this, many enterprises have abandoned conventional records management and archiving procedures in favour of a relatively cheap and fast backup procedure. The organization of the data mirrors the computer's structure, not the human records management structure; therefore it implies cost and time in retrieving.

2.2.6. Legacy data and systems

Paper based documents regardless of age, can usually be read and understood on site, though there may be some damage by water or fire etc, they are seldom written in a dead language.[25]But it is common to find that old data are impossible to read using current hardware and software. Or old data transferred to current media and format has lost important elements necessary to establish context or authenticity. Computer applications are upgraded constantly. They quickly become obsolete. In the context of civil litigation, enterprises that have taken backups on a regular basis, perhaps storing one per month for the past twenty years, face the doubly daunting task of having to expand resources to restore the backups to useable state, and then search the disorganized files, before they can determine whether or not the backups contain any data relevant to the litigation.

3. IT assistance in the management

An organization needs to take steps to be prepared for discovery of its electronic systems. If an organization waits until it is involved in the litigation, before closely analyse what is stored in its electronic system, and then prepare for the discovery, it may be too late. Technical and legal personnel need to conduct

24 Back up: to create a copy of data as precaution against the loss or damage of the original data.

25 This is compared with the computer application or language, which usually develops much more quickly than the common language. For example, a paper document written 15 years ago using common language can easily be read and understood, while a computer program of 15 years age may be impossible to use in the current application.

a review to sensitise the organization to the risks involved in its conduct.[26] Several types of technical tools are available to help managing the electronic discovery, limit cost and delay and if necessary, resolve discovery disputes.

3.1. Security and integrity

As we have mentioned above, electronic document can be altered, destroyed or manufactured in a convincing way by even novice computer users is alarming. The issue of security and integrity[27] of information on electronic media are therefore closely related. Sufficient security procedures must be in place in order to ensure the integrity of the information stored in the electronic system. Technically speaking, first, it helps to determine the source or origination of a document as well as whether a document has been altered after it is initially stored on an electronic media which is also usually referred to as the authentication of data. Second, it helps to ensure the structure and logic correctness of data, which other wise may be affected due to the intentional damage by hackers or accidental system failures etc. Furthermore, for possible legitimate use as discovery, the completeness, accuracy and validity of data, is also relevant, and need to be ensured.

In the legal sense, information security refers to the legal obligations concerning maintaining or enhancing the technical information security and to the measures required by law to protect and promote efficiency of the information required at court.[28] Vice versa, "the efficiency of the legal rights is also dependent on the quality of technical infrastructure."[29] In addition to the legal rights the information security and sound arrangement of the infrastructures are necessary for the taking into account of the user's rights and interests of the other persons and parties. The security issue is thereby linked to the effective management of electronic data, and should be the first step we take for the management of electronic discovery.

---

26 Daniel F. Perez, Exploitation and Enforcement of Intellectual Property Rights, 10 Computer Law, Aug.1993, at12.

27 Integrity refers to the qualities of data and data processing being reliable, authentic in relation to the original data, structurally and logically correct, valid and complete, and to the non-repudiation of communication and data processing acts.

28 For example, according to the Federal Civil Litigation Rules, organizations have the obligation to ensure the availability and integrity of the data that may become the discovery required in the foreseen litigation. We will return to this later in the paper.

29 Tuomas Poysti, Information Security Commentary, available at http://www.uroa.fi/home/oiffi/enlist/commentary/information_security.html, Context Ltd., 2000 (last visited Jan 9,2002).

In the following section, we will provide some methods for improving the security of an organization's computer system. While these methods may serve as a framework for expert testimony regarding the integrity of a particular document, these guidelines are not intended as a method to provide a sufficient showing of the condition precedent required for admissibility in court.[30]

3.1.1. User ID and password

Passwords are often the first (and possibly only) defence against intrusion,[31] which accordingly is the first security gate for ensuring the authentication of the data stored and transmitted in the computer system which is essential for the validity of electronic discovery at court.

They protect information that we don't want anyone to know. Passwords are cheaper than other more secure forms of authentication like special key cards, fingerprint ID machines etc. They are generally used in combinations with some forms of identification, such as user name, account number, or e-mail address. While a username established the identity of the user for the computer or system, the password, which is known only to the authorized user, authenticates that the user is who he or she claims to be. This means that their function is to "prove to the system that you are who you say you are".[32] They are designed to make it harder for an unauthorised user to alter existing documents or to forge a message. Therefore, they are gateways to improve the authentication of the data, which is at the core of maintaining the quality of the information that may subject to the discovery.

However even with the implementation of the user ID and password systems, it is still possible that the person holding the password may disclose it intentionally or unintentionally, or a hacker can determine the user ID and password of an authorised computer user, and a security breach may occur. Passwords can be cracked in a variety of different ways. [33] Numerous cracking tools that an average person can use are also available.[34] Therefore it is necessary to follow some security rules to reduce the risks.

---

30 See FED.R.Evid.901.

31 Mac Gregor, Tina: Password Auditing and Password Filtering to Improve Network Security, SANSCA,

1991&1996, last visited April 18, 2003, available at (http://rr.sans.org/authentic/improve.php).

32 Russell, Deborach and Gangemi Sr., G.T.: Computer security basics, O'Reilly &Associates, Inc.Sebastopol, CA, 1991.

33 Cf further for password cracking at www.passwordportal.net

34 Cf further for password cracking tools, the Security Focus article, Password Crackers-Ensuring the Security of Your Password at Http://www.securityfocus.com/printable/infocus

It is often recommended that the password in use should be a combination of letters, numbers, and punctuation marks instead of just a word from dictionary or the user's name or birth date etc. However this may increase the possibility of forgetting the password the creator himself. "A good password is easy to remember, but hard to guess."[35] Using mnemonic phrases that have personal meaning, or taking the initials of each of the words in that phrase to convert some of those letters into other characters, are common ways of creating a good password. For example submitting the number 3 for the letter "E", or spell phrase phonetically such as "ImaKat!"(Instead of I'm a cat!) Or using the first letters of numerous phrase such as: "Swfihh&"= "Smile with flowers in her hands".[36] Besides this, extra protections are also needed. Such as users should be required to change their password periodically. The system should not allow additional log on attempts for at least five seconds if the user ID and the password do not match on three consecutive logs on attempts.[37]

3.1.2. Firewalls

A firewall is software or hardware that limits access to a computer from outside sources, and examines packets of information sent to the computer over the Internet. Good firewall software also examines the packets the computer sends to the Internet.[38] The firewall decides whether to accept or reject a packet based on rules that examine a packet's source and destination address, port number and contents. If a packet matches the criteria in the rule, the software takes action. Examining outgoing packets is as important as monitoring the packets that come into the system. A "Trojan horse"[39] can initiate the communication of personal information, such as user names and passwords, from

35 Armstrong, Del and Simonson, John: "Password Guessing" and "Password sniffing", An Intro to Computer Security, School of Engineering & applied Sciences, University of Rochester, Oct.25, 1996. http://www.seas.rochester.edu:8080/CNG/docs/Security/security.html

36 Cf further see University of Michigan, Information Technology Division, Password security: A Guide for Students, Faculty, and Staff of the University of Michigan, Reference R1192, Revised April 1997. http://www.umich.edu/~polices/pw-security.html

37 Id.

38 Diana Lawlwss, Bits & Bytes, Official News Letter of the Tampa Bay Computer Society, last visited May 9 2003, available at:www.tampa-bay.net

39 "This is a destructive program that masquerades as a begin application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. The term comes from a story in Homer's Iliad in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojan drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture troy." Cited from www.webopedia.com/TERM/T/Trojan_horse.html

your system to an unauthorised individual. A firewall is necessary if the LAN within an organization is allowed to communicate with computer outside the organization, for instance by accessing the Internet. A firewall involves a computer running a specialized software application that controls the flow of information.[40] The firewall may enforce specific policies such as to disallow all login traffic from the outside or requiring a specific security clearance before allowing login from the outside.

Additionally, a firewall may include a logging system that records information such as user ID and time of day. Such logging systems may also be set up to record all the information that is communicated through the firewall.[41] And this time stamp function (provided the time is accurate) of firewall can be of great value when it comes to prove the authentication of electronic discovery. Since in the ordinary security protection such as the digital signature,[42] password system, can only bind "who" (the signer) with the "what" (the digital data), but leaves a question unanswered: How long after the digital evidence was seized, was it integrity protected? For this question, time become a critical factor in proving the integrity of electronic discovery. As a qualified value, time is used nearly in all aspects of commerce and security in order to bind validity and reconstruct the order of events. Adding secure time[43] to electronic discovery eliminates the potential for fraud and unintended errors. The use of secure date/time stamps cannot only improve the integrity of electronic discovery, but also provide higher assurance required for digital chain of custody.

3.1.3. Encryption

If an organization determines that an added level of security is necessary, the organization could require encryption of documents before they are transferred or stored. For this purpose a so-called Public Key Infrastructure (PKI) has been developed. The purpose of an open key system of this sort is to let a reliable party issue an electronic certificate identifying the signatory to a given

40 Id.

41 Similarly, the routers used to direct information across the Internet, for example e-mail, may also record all the information that is being sent, this internal correspondence between two offices of the sae company via the Internet could be recorded in a variety of locations along the transmission path.

42 We will return to this later.

43 It has been suggested that the time stamp should be secured and even notarised by a third party, to ensure the integrity of electronic discovery. And secure, auditable time should be added to the electronic signature. In this paper we will not deal with this too much. Cf.further Chet Hosmer, President& CEO WetStone Technologies, Inc. Proving the Integrity of Digital Evidence With Time available at http://www.ijde.org/archives/chet_article.html (last visited May 5,2003)

electronic signature. Simply speaking, electronic signature has a bearing on the content of the encryption, and it is in fact a result of harsh sum algorism. The certificate focuses on the identity of it and links the signature to person. Proving that who made the electronic signature is who he declares to be by an electronic document.

There are two main types of certificate one is soft certificate which can be stored in the computer user's hard disk, the other is hard certificate, which can be saved on an independent storage device usually called "smart card". When it is used the card must be inserted with a activate password. The next step is to calculate the so-called harsh sum regarding the amount of information that shall be signed. This is done with the help of a special algorithm, which results in a kind of "electronic fingerprint". After that the hash sum is encrypted by means of the user's private cryptographic key, the result is an electronic signature. The user may send off the amount of information together with the electronic signature and his personal certificate. The recipient receives the amount of information and calculates a new harsh sum. The e-signature can then be decrypted because the recipient has received access to the provider's open key in a secure way. Both hash sums can then be compared and if they tally, the recipient knows that no distortion has occurred. In order to check whether the sender's identity corresponds to the real one, (and whether the card has not been frozen) the provider of the certificate need to be contacted. [44]

This kind of encryption binds the sender's identity to the integrity operation, and prevents unauthorized regeneration of signature unless private key is compromised. Which therefore is recognized as a more secure way of realising confidentiality, and authenticity of electronic information stored and transferred in the computer system. Accordingly, it ensures the integrity of electronic discovery originated from this system.

3.2. Litigation support software

In order to track, analyse and use the voluminous digital data, using some litigation support program to build a database is a common way of management. For cases in which you might expect to find hundreds or thousands of documents, a litigation database of some sort is almost mandatory. There are a number of well-designed database products on the market that are classified under the title of "litigation support software". They act as a filter to help us

44 Cf. further Cecilia Magnusson Sjöberg, Electronic Signatures-Measures Required Despite a New Law, Development and Management of Information Systems in a Legal Perspective, and Stockholm 2001 at 771.

sharply focus upon what we have in our case while reducing redundant or distracting documents and information.[45]

Filtering out discovery "noise" was hard for anyone doing traditional manual discovery. If one had a few hundred thousand documents to review, the process might take years and it is still highly likely that one would either overlook the most important documents or perhaps miss their significance and relationship to other discovery materials. Poor management of electronic discovery results in the liability to access necessary information and a lack of control. The electronic information must be kept in such a way as to make them findable and usable. This requires manual indexing or text retrieval.[46] Selected segments of information are recorded such as metadata, author, recipient and nature of document… The information is linked to the documents in a number of ways. By using this method, the information retrieval of the electronic discovery becomes more efficient than before.

3.2.1. Manual indexing

Modern indexed search program using Boolean search functions[47] and enhanced by thesaurus-based searching[48]speed up searching while assuring a much more comprehensive search. Rather than entering the full text of a document, it is indexed or summarized by a computer using key terms or fields, and then entered into the database in that format. The computer then searches through the database to identify documents using those key terms. The terms can be assigned manually.

An effective index must characterise the information contents of stored documents through terms in the index. In a product liability case involving a particular design defect, an effective database would contain a specific field

45 In fact, the litigation support software can not only just filter out information, but also have other functions such as electronic calendar, electronic distribution, tracking task, assignments and events, billing building system etc. As the paper focus on the management of e-discovery, which is closely related to the document management, the other functions will not be dealt with. Cf. further Delaware State Bar Association, Tips on Technology, www.blankrome.com/publications/articles/ (last visited May 5 2003)

46 Strictly speaking, text retrieval also uses indexing, but it is generated automatically by the computer.

47 "Boolean"-a retrieval system based on a combination of words and operators. Boolean systems use operators such as "and", "or" and "not". The operators and search words combine to target documents in a database, which do or do not contain a give set of words. Cf. further, Karlgren, Jussi, The basics of Information Retrieval, Statistics and Linguistics, Development and Management of Information Systems in a Legal Perspective, Stockholm 2001 at 208.

48 It means the computer's can search some word close to the same meaning or spelling, not just exactly the same word. We will return to this later.

noting any documents that relate to any aspect of that design. If it involves a mental damage, for example, it would be important to enter the word "mental damage" as a key term for any documents that specifically refer to the "mental damage" in question. Ideally the index represents the information contents of the stored documents.

Manual indexing are judged by human information experts and assigned with terms from predefined vocabulary[49] that they think characterise the contents best; usually they can best be trusted to extract the intended meaning of a text and describe it with the best characterising terms. However humans are not consistent in the selection of the index terms they assign,[50] and the Indexer has to choose what perspective to use and hope the user makes the same choice. The information accordingly turns out to be subjective. One other problem, which makes the index describe the information contents of documents only partially, is due to the limited semantics of the language. Even if we assume there is agreement as to the meaning of a document, a limited set of terms dose not suffice to fully describe it. And that is why some advanced information retrieval system uses more complex index languages.

3.2.2. Text retrieval

Text litigation support system uses OCR technology[51] and other applications to allow the attorney access to an entire transcript or document through text and retrieval techniques. The most common application of text litigation support is the preparation of deposition transcripts on disk, CD or hard drive. With the this, the attorney is able to use computerized retrieval programs to search one or more transcripts for every instance in which a particular name or phrase is mentioned, rather than going through the time-consuming process of manually searching for that information in the transcript.

Provided the document is originally in paper form, OCR technology improves and becomes more reliable and cost effective, the ability to conduct text searches may eliminate the need for manual indexing. Several litigation support programs are available that are capable of automated creating an index of every word in a document, with cross-reference to the location of the word in the do-

49 There are certain rules for selecting the terms in order to applying them consistently and maintaining the vocabulary. So the selection is not totally free, however it still causes some problems that we will touch upon later.

50 Cleverdon, C.W. Optimising Convenient Online Access to Bibliographic Database, in Information Services and Use, Vol.4 (1984) nr.1/2 (April) p.37-47.

51 Optical Character Recognition software, scanning documents into a database minimizes the problems associated with lost or misplaced files.

cuments. Compared with the manual indexing, this is faster and requires no human intervention. Whereas a text search conducted through a traditional word processing program can only search for a single word or phrase and "hits" every appearance of the word, regardless of the context. With such programs, the time saving aspect of building a database is severely limited; not much time is saved if one is only able to search for one word or phrase and that search reveals thousands of documents.[52] More sophisticated litigation support software allows for more complex search configurations in a full-text database, such as "Boolean" and "fuzzy" searches,[53]concept search,[54] or probabilistic retrieval.[55]

3.2.3. Text search and manual indexing

As we have pointed out both the manual indexing and the automated text retrieval have their advantages and drawbacks. As indicated, the solution will be choosing software that combine the two techniques and avoid their drawbacks.

Program with some functions such as adaptive pattern recognition (APR) or fuzzy search capabilities allow the lawyer to search for the misspelled words in a database. The APR software assumes that is looking for the closest match to the entered search requests, not necessarily an exact match. Depending on how sensitive the software is set; ranked "hits" are returned. The best or exact matched are at the top of the list with less matched results listed below.

If the index has been carefully constructed, an indexed search hits only those instances in which the word is used in a specific context. The trade off in using text versus indexed searched, therefore, is between quantity (i.e. the total universe of documents in which the word may be found) and quality (i.e. finding only those documents that are on point). In a complex case that with piles of files, relying entirely on text searching is generally impractical, since it requires OCR scanning of every document unless it is originally stored in electronic form. And for some other types of document with pictures or handwriting, even the OCR technology cannot help. On the other hand indexing manually is also not practical for people responsible for it. Moreover, due to new insights and the development of the legal system, the topics that used to be crucial before may become irrelevant afterwards. In most cases, it is best to reach a balance

52 Cf. further, Curran and Higgeins, a Legal Information Retrieval System, 2000 (3) The Journal of Information, Law and Technology (JILT).

53 "Fuzzy" locates words that look similar to the selected word. Cf. further Id.

54 A search for document related conceptually to a word, rather than specifically containing the word itself.

55 Which rank the retrieval documents by likelihood of providing relevant data for the resolution of the information request as expressed by the search terms.

between both, words-scanning of those "hot documents" that are most likely to be key to the case, and indexing those that are more basic.[56]

3.2.4. Selecting the litigation support software

Determining which program offers a particular practitioner the best solution for handling document-intensive cases is a task that arises frequently, particularly because the use of automated database litigation support is on an exponential rise.

Basic concerns

The most important principle is to understand that the computers can only assist in placing information in the hands of the lawyers. Even the most sophisticated software will be useless in an untrained hand or mind. If one wants an effective computerised litigation support for managing the electronic discovery, one must know how to control the system from the beginning, and be clear what one needs. Once the goals are established, communicate them to the technical expert who will supply both the equipments and work, and help us to understand what exactly we want to accomplish. This is costly, but in the long run may serve costs and time. If one dose not understand how the data is classified and stored, it will be difficult for one to find it.

To use computerized litigation support effectively, an understanding of the case and the law involved is necessary. If the case is so document-intensive that temporary personnel or outside contractors must be used to help summarize and enter documents into database these people must be educated with the facts of the case. Lack of knowledge about the case could mean that key documents get overlooked.

Having identified the needs, the practitioner can start to choose the software. Usually the first issue that need to be taken into account is its compatibility or ability to interface and link with existing hardware and software installations. Greater compatibility with the existing programs may require a trade off in reduced functionality. For example, a fantastic database management system with great "bells" may not interface with the word processor and spreadsheet application, and therefore may prove to be more of a hindrance than help.

When it comes to choosing the actual software the following factors may need to be taken into considerations: Is the program user friendly (easy to use and install)? How about its search function? Can it be expanded? Can it

56 Cf. further Luuk Matthijssen, Interfacing Between Lawyers and Computers, at 19-30,Katholieke University, 2000

link to other kind of programs or third party software? Is it easy to import or export something like transcript? How about its portability features? Usually there are no software that can fulfil all the requirements of the users, they all have their own pros and cons, therefore it is important to choose the appropriate one for one's own needs, and make sure the pros of a certain product is more important than the cons of it for you.

Categories of software

Different software often has different characteristics,[57] in order to choose the most appropriate software; it is necessary to get some idea about the specialities of different software. For example, for small to medium case, CaseMap 4, along with its associate time line program TimeMap(see figure1), are particular flexible means of organizing discovery, understanding significant time lines, and using the resulting data at trial.

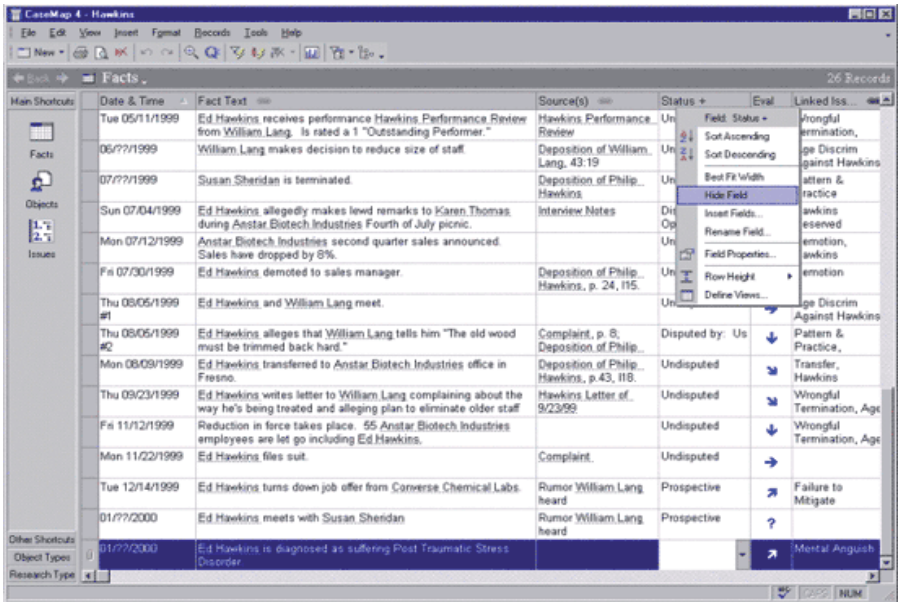


Figure 1 the interface of CaseMap has direct link to the TimeMap

57 Cf. further Law Computing available at http://www.lawofficecomputing.com (last visited May 9, 2003)

It also integrates with Adobe Acrobat ®, Summation, LiveNote, Concordance, Binder, Opticon, Doculex, Sanction, Trial Director, and other software products. If you have scanned or imaged any discovered electronic and paper discovery, you'll be able to directly associate a PDF file (if the document is in this format) of each discovered document directly with its CaseMap or TimeMap entry and call up the imaged document with a single click within CaseMap by using a standard program such as Adobe Acrobat. It is a fast and neat way to work with the discovered documents.

If you are dealing with many possible actors and large quantities of information, then an industrial strength management system such as IBM's Lotus Discovery Sever 2.0. (Now in version 2.0.1),[58] will greatly reduce the manual efforts otherwise needed to identify and model information flow within a large entity. It includes Kmap, which is a graphical representation of an organization's knowledge (see figure2). The K-map is the backbone of the Discovery Server search-and-browse user interface. From the K-map interface, you can locate content from many disparate sources, by drilling down through subject categories, using full-text search, or using a combination of both search strategies. Additional information about the relationships between people and document activity adds value and context to the user's search and retrieval experience. Because the K-map displays related documents, people, and places in categories, users can browse and search for information in context.[59]

58 Cf further Lotus Discovery Sever 2.0.1at http://www-10.lotus.com/ldd/today.nsf/0/3c06ffb3253066b085256cbd0045cdce?OpenDocument (last visted June 20,2003)

59 Cf further Lotus Discovery Sever 2.0 at http://www10.lotus.com/ldd/today.nsf/9148b29c86ffdcd385256658007aaa0f/ea27b7f8979c99ac85256b9d00030b29?OpenDocument (last visited June 20,2003)

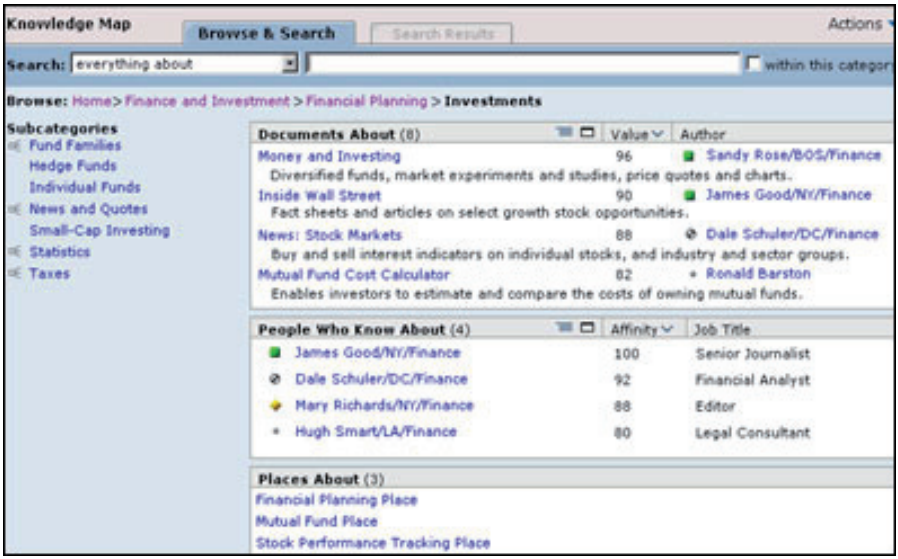


Figure 2 Kmap building Service

Programs like discovery Sever 2.0. automatically sort through the discovery target's electronic systems for relevant information, identify potentially rich "nodes", which may be particular authors, recipients, departments, or document types, and then map the relationships between the potentially most profitable target for more focused discovery. This offers significantly enhanced administration functionality. It lets the user have greater control over installation, set up, and maintenance. And users will have a better idea of what's going on "under the hood" of Discovery Server. However the resources to do this sort of highly automated discovery will be expensive and will require counsel to formulate reasonable ground rules.

Data mining software, often but not always used on mainframe computers, is also potentially useful in making sense out of large masses of otherwise undigested data. Some well-established data mining software, such as SPSS (now in version 11.5), worked statistically with numerical data. Other knowledge management programs, such as Lotus Discovery Server, discover and group related textual documents. The ability of discovery Sever to map the relationship between individuals and clusters of potentially pertinent documents makes it a very powerful electronic discovery tool in highly complex corporate and organizational situations, but setting up and using this tool requires experience and technical knowledge that's beyond most attorneys.

4. Legal Management tools for electronic discovery

The ability to use the advanced technology is indispensable for effective management of electronic discovery, but the process goes well beyond simply using technology. The practitioner needs to be a legal professional also in order to solve the legal problems involved and avoid an impasse. In the following part we will discuss some most frequently cited federal rules when it comes to the cases relevant to the electronic discovery. And we will try to explore how the rules can be used as tools by the legal professionals for effective management.

4.1. Discoverability and admissibility under the federal rule

"Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action…"[60] Thus, as a general proposition, the federal rules do not discriminate between electronic and paper data. The usual vehicle to acquire electronic data is a Request for Production of Document and Things under Rule 34,which states:

> *Any Party may serve on any other party a request (1) to produce and permit the party making the request…to inspect and copy, any designated documents (including writings, drawings, graphs, charts…and other data compilations from which information can be obtained, translated, if necessary), by the respondent through detention devices into reasonably usable form*[61].

The 1970 Advisory Committee Note to Rule 34 has been quoted extensively as further support for the proposition that computer data is discoverable. It states that:

> *The inclusive description of documents is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detention devices and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into*

60 FED.R. CIV.P.26 (b) (1)
61 FED.R. CIV.P.34 (a)

usable form. In many instances, this means that respondent will have to supply a print out of computer data.[62]

The computerized data has been widely accepted as a part of the "document" discoverable in the court. In Crown Life Ins. Co. v. Craig plaintiff failed to produce raw data from its electronic databases. The Seventh Circuit stated that "while it may be true that the plaintiff could not access the data at the time of the request, that dose not mean that the data did not exist or was not discoverable. The plaintiff had a duty to make the data available to defendant".[63] The court cited the Advisory Committee Note as support for the proposition that data, even data that never existed in hard copy form, is considered a "document" under Rule 34.[64] Legislation and interpretive jurisprudence leave no doubt that electronic data is discoverable and may become admissible evidence. It is important to understand the basis on which one can avoid risk or sanction that based on this rule.

4.2. Legal tools for electronic discovery management

4.2.1. Pre-trial conference

Perhaps the most important legal management tool in electronic discovery cases is the Rule 16(c) pre-trial conference. Rule 16 (c)[65] of the Federal Rules of Civil Procedure[66] lists several issues that may be addressed during the pre-trial conference, and it is possible for the judges to add some additional points like electronic discovery and issue a memo to the attorneys before the conference. The purpose of the Rule 16 notice is to save the parties time and expense by anticipating the most common issues of electronic discovery, developing a reasonable discovery plan, and avoiding unnecessary conflict.

---

62 Id. The section of the note that is quoted less often states: "The burden…placed on respondent will vary from case to case, and the courts have ample power under Rule 26 (c) to protect respondent against under burden or expense, either by restricting discovery or requiring that the discovering party pays costs."

63 Id. at 1383 cf. Fautek v. Montogomery Ward & Co., 96 F.R.D.141 (N. D: III 1982) (holding failure to produce code book needed to read and understand computer tape should be punished with discovery sanctions).

64 Id. at 1382-83; accord in re Air Crash Disaster at Detroit metropolitan Airport, 130 F.R.D.634 (E.D: MIch.1989); Dunn v. Midwestern Indemnity Co., 88 F.R.D.191 (S. D: Ohio 1980).

65 FED.R. CIV.P.16 (c)

66 Cf. further the Federal Rules of Civil Procedural of the United States at: http://www.law.cornell.edu/rules/frcp/overview.htm (last visited June 15, 2003)

However, it would be frustrating experience if the opposing counsels attending the conference do not know what their client has or can produce in discovery. Though it is true that attorneys cannot be expected to become computer experts for the purpose of discovery and should not do so. It is usually advisable to encourage communication between the people who actually know the respective computer systems. The information such as which computer systems were in place during the period of time relevant to anticipated discovery; the extent of the computerized information (including back ups and archives) that will need to be searched in the course of discovery; the capability of each party to perform searches and produce material in a useable format; the security measures being taken to preserve the potential computer evidence; may be needed to be taken into account beforehand.

4.2.2. Initial disclosures

Under Rule 26(a) (1),[67] the parties must unilaterally disclose the existence of relevant documents and other categories of information before receiving a discovery request. The scope of document disclosure found in proposed Rule 26(a)(1)(B)[68] has been narrowed from documents "relevant to disputed facts alleged with particularity in the pleadings" to documents "the disclosing party may use to support its claims or defences." In the same round of amendment proposals, the Committee reinforced Rule 37 (c) (1)[69] to make it clear that a party is not permitted to use evidence at trial, at a hearing, or on motion that was not disclosed initially or included in an original or amended discovery response.

While the Rule 26 initial disclosure may be viewed as a device to expedite attorney-managed discovery, it may also be viewed as a judicial management and dispute resolution device. It can force the attorneys to investigate the factual basis of their case or defence early, before the first rule 16 scheduling conference, allowing them to provide the judge with a much clearer picture of what formal discovery in the case might involve.[70] Initial disclosure under proposed Rule 26 (a) (1) (E) will require that attorneys undertake a reasonable investigation of their client's computer files and disclose computer-based evidence that they may use to support their claims or defences. Failure to do

67 FED.R. CIV.P.26 (a) (1)
68 FED.R. CIV.P.26 (a) (1) (B)
69 FED. R. CIV.P.37 (c) (1)
70 See e.g. Clonley & Hodge Associates, Manual for Pre-Discovery Disclosure (1994), interpreting the local rules and practice in the District of Massachusetts, which closely followed Fed.R.Civ.P.26 as adopted in 1993

so may face the sanction under Rule 37(c)(1). In order to do the investigation, some technical support such as an efficient information retrieval system will be very useful. It will even be helpful if a good litigation support software such as the Lotus Discovery Sever 2.0 had been adopted in the organization, whose Kmap will provide a clear graphical representation of all the organization's knowledge stored in the computer system.[71] And it would be more effective if the company had undertaken appropriate retention policy that ensures an effective management of the electronic information in its computer system.[72]

To some extent, Rule 26 is closely linked to Rule 16, and it will undoubtedly become a subject of discussion in the pre-trial conference if the parties fail to reach an agreement on the scope and conduct of discovery beforehand. As such, it may enable both the judges and attorneys to weigh the benefits and burdens of discovery, shift the cost of discovery etc.

4.2.3. Resisting discovery

As a general rule, a party is entitled to discover information that is relevant to the subject matter in a pending action unless it is overly broad, unduly burdensome and harassing. Under the current Rule 26, the trial court has the power to limit the discovery, and it can also be used as objections the responding party can take to minimize the possibility of production of the entire computerized system even after litigation has commenced. The current Rule 26 (b) (2) (i), (ii) and (iii) citing the "information explosion of recent decades which has greatly increased both the potential cost of wide–ranging discovery and the potential for discovery to be used as an instrument for delay or oppression".[73] A further amendment to Rule 26 (b) (1), stating that "all discovery is subject to the limitations imposed by subdivision (b) (2) (i), (ii) and (iii)."

---

71 We have talked about this before in Section 3.2.4.

72 We will return the retention policy later in Section 4.3.

73 The proposed Rule 26 (b) (2) reads as follows: "(2) limitations, By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30.By order or local rules, the court may also limit the number of requests under Rule 36 .The frequency or extent of the use of the discovery methods of otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive;(ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or,(iii)the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26 (c)."H. R. DOC: No.106-228.at19 (2000)

Rule 26 (b)(2) (iii) provides the instrument to limit the burdensome discovery. In the case Fennell v. First Step Design[74] the plaintiff's propose for discovery was denied after the parties could not agree on a protocol that would reasonably determine whether the plaintiff's claim that the memo had been altered was true, and an appropriate scope of the discovery. And the appealing court cited both Rule56 (f)[75] and Rule 26 (b)(2)(iii) and went into depth on the risks and cost involved, the likelihood that the proposed discovery would not result in any significant new information, concluding the trail judge did not abuse his discretion in denying the plaintiff's request.

Besides proposing for the limitation from the judge by using the listed factors in the Rule26, parties involved can also take actions as following to resist the excessive discovery.

> *Provide only printouts of documents stored in electronic media; require the requesting party to specifically request electronic form prior to a production in an electronic form;*[76]
>
> *Where the requesting party asks for computer-readable form, do not reveal any more than is necessary about the system.*[77]
>
> *Assert the production of electronic information in a "native" form would violate the attorney-client privilege or expose protected work product in that the organization of the document or the directory structure would reveal such protected information.*[78]

In addition, it is also important to take time to delete the obsolete data in the computer system in order to avoid the excessive discovery liability in litigation. However people usually tend to forget to take some time to delete the obsolete files in their computer system, which may cause great troubles in the future litigation. Some litigation support software may have the relevant function. For example, DTS File Bulter can delete the obsolete files efficiently. Simply by adding the deletion date to the filename when the file is created and run the File Bulter over a coffee break, lunch, or at night, it will quickly either delete or move obsolete files. This function cannot only eliminate the possibility of the

74 83 F.3d 526 (1st cir.1996)

75 The computer inspection in this case was proposed in the context of pending Rule 56 summary judgment motion after formal discovery was closed, and the appeal court based its decision on the procedural posture of the case as well as the merits of the proposed discovery.

76 John T. Soma& Steven G. Austin, a Practical Guide to Discovering Computerized Files in Complex Litigation, 11 REV: LITIG.501, 519 (summer, 1992).

77 Supra note 48.

78 Id.

legal exposure we mentioned, but also solve problems such as: the computer getting loaded up with unwanted files, longer back up times, requirements for more expensive backup system, and greater difficulty finding documents that one needs etc.

4.2.4. Cost bearing

Electronic discovery may involve extraordinary costs that are clearly outside the usual cost of doing business. In Anti-Monoply v. Hasbro[79], the defendant stated that the data requested by the plaintiff could be extracted from its database only by special programming techniques. Otherwise, the defendant would be forced to give the entire database over to a competitor. The court required the plaintiff to pay the defendant's reasonable costs to produce data in digital form. In another case Brand Name Prescription Drug Antitrust Litigation,[80] the cost to the producing party of searching 30 million e-mail messages for relevant information, estimated at $50,000 to $70,000, was held not to be "undue" and would not be shifted to the requesting party.

When faced with the issue of who should bear the cost of producing a printout of digital records, courts have increasingly required the responding party to bear the cost of producing electronic data.[81]In the case Bills v. Kennecott Corp[82] the court offered four factors to consider in determining whether to shift the costs of discovery from the responding party to the requesting party:

- Whether the amount of money involved is not excessive or inordinate;
- Whether the relative expense and burden in obtaining the data would be substantially greater to the requesting party as compared with the responding party;
- Whether the amount of money required to obtain the data as set forth by the responding party would be a substantial burden to the requesting party, and
- Whether the responding party is benefited in its case to some degree by producing the data in question.[83]

In the Bills, court ordered both parties to pay a portion of the costs associated with producing e-mail form digital data. This as I see is better than forcing the

79 1996 WL 22976 (S.D.N.Y.)
80 1995 WL 3360526 (N.D. III.1995)
81 Charles A. Lovell & roger W. Holmes, The dangers of E-mail: The Need for electronic data Retention Policies, 44 R.I.B.J.7, 9 (1995).
82 108 F.R.D.459,461 (D. Utah 1985).
83 Id.

responding party to shoulder the costs of producing whatever the requesting party demands. Furthermore, that the responding party is in a better position to conduct the production should not mean that it is in a better position to pay for the production.

It is within the court's discretion to fashion a cost-sharing procedure for large–scale electronic discovery. For example, in addition to the factors listed above, the court may consider the parties ability for payment, this factor would constitute a check on abuse of the discovery process, especially where the opposing parties are of financially disproportionate means. Simply put, this approach could avoid the unfair result of a party prevailing by outspending the other party, rather than on the merits of the case.

4.2.5. Request for production

Rule 34(b) if the Federal Civil Litigation Rules states, "a Party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the requests."[84] The quoted language was added to Rule 34 in the 1980 amendments to the Rules. The purpose of adding this language was to address the problem raised by some parties who were engaging in the needle-in-a-haystack methods of hiding critical or damaging documents in a large mass of unrelated materials in an attempt to obscure their significance.[85]

In case Kozlowski v. Sears, Roebuck& Co.,[86] the defendant interpreted "as they are kept in the usual course of business" as meaning producing everything in their files whether relevant or not in response to the discovery requests. In interrelating Rule 34, the court stated that:

> *The defendant may not excuse itself from compliance with Rule 34,Fed. R.Civ.P., by utilizing a system of record keeping which conceals rather then disclose relevant record, or makes it unduly difficult to identify or locate them, thus rendering the production of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generate filing system, and then claiming undue burden, would defeat the purpose of the discovery rules.*[87]

84 FED.R.CIV.P.34 (b).
85 FED.R.CIV.P.34 Adversary Committee's notes.
86 73 F.R.D.73 (D.Mass.1976).
87 73 F.R.D.73, 76 (D.Mass.1976).

Using the methods prescribed in Rule 34, it is clear that a responding party may not deluge a requesting party with numbers of documents that are not requested. Instead, Rule 34 requires the responding party to find the documents that were sought. In the case of information stored in electronic form, unless the requesting party seeks to discover and has the right to discover the entry of the electronic discovery, a responding has the duty to select the relevant information. The data mining software SPSS 11.5 we mentioned before maybe very helpful here. It has the new TwoStep Cluster analysis technique to get the most accurate identification of clusters in user's data. This state-of-the-art algorithm allows the user to find clusters in very large datasets. And mix datasets with continuous (such as income) and categorical level variables (such as job type).[88]

A massive volume of documentation, whether relevant or not, can be generated in a short period of time. And each member organization generally creates its own electronic filling system. Though these systems may seem logical from the creator's own perspective, it is unlikely that other people using an identical system can understand it, not to mention the outsiders. For the proper presenting of the electronic discovery, it is essential that court strictly enforce Rule 34. And it is also important for the attorneys to inform their client about this rule when responding with electronic discovery.

4.3. Retention of electronic discovery

An organization must be careful when destroying any type of document; destruction of evidence may lead to an adverse inference under the doctrine of spoliation. State or federal law might subject an organization to an "affirmative legal requirement" to keep certain records for specific time periods.[89] Rule 37 of the Federal Rules of civil procedure; impose discovery sanctions to control bad-faith destruction of documents pursuant to the rule. It is applicable to the 'normal' disputes, delays or difficulties occurring in civil litigation. Its sanctions are appropriate in instances of a litigant's failure to make or cooperate in discovery. Rule 37 enables a court to punish the litigant who has not responded adequately to discovery requests of an opposing party or to orders of the court compelling discovery.[90]

88 Cf. further at www.spss.com (last visited June 20, 2003)

89 See Henery E. Knoblock &Christopher J. MacKrell, Sample document Retention Guidelines, American Corporate Counsel Association, Records Retention Manual, 1995

90 Capellupo v. FMC Corp., 126 F.R.D.262, 265-67 (W.D.La.1982).

4.3.1. Acknowledging a reasonable standard

It is true that society has an interest in imposing upon organizations an on going obligation to retain documents potentially relevant to current or future litigation,[91] organizations have a legitimate interest in the destruction of unnecessary records/documents. To balance the two interests a reasonable standard is needed.

In Lewy v. Reminto Arms Co[92] the court reviewed a document retention program[93] implemented by the defendant corporation. On appeal, the defendant argues that the general instruction given to the jury by the trial court judge was inappropriate, The instruction provided: "If a party fails to produce evidence which is under his control and reasonably available to him and not reasonably available to the adverse party, then you may infer that the evidence is unfavourable to the party who could have produced it but did not".[94] The plaintiffs had requested the imposition of the instruction when the defendant was unable to produce several documents that had been destroyed pursuant to the defendant's document retention policy. The defendant, however, argued that the destruction took place pursuant to routine procedure and thus could not result in an adverse inference.[95]

In remanding the case, the Lewy court set forth a number of factors, which the trial court was to consider if the lower court was again called upon to impose sanctions arising from the defendant's implementation of a document retention program.[96] The trial court was asked to first "determine whether (the defendant's) record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents." Then consider the extent to which the destroyed documents were relevant to pending probable lawsuits. Finally, the Lewy court instructed the trial court to consider whether the document retention policy was instituted in bad faith.

---

91 Society also has an interest in the promotion and maintenances of the right to privacy. Cf. further Judith Wagner DeCew, In pursuit of Privacy: Law Ethics, and the Rise of technology (1997).

92 836 F.2d 1104 (8th Cir.1998); see also Peter v. Lacouture, discovery and the use of computer based Information in Litigation, R.I. B.J.Dec.1996, at 9,11 (examine the standard outlined by the Lewy court)

93 A document retention program involves the systematic review, retention and destruction of document received or created in the course of business. Cf. further Daniel S. Hapke, jr., Developing and Implementing Records Retention Programs in Business Organizations, American corporate counsel association, records Retention Manual 1995.

94 Id.

95 Id.

96 Id.

In addition to consider the nature of the destroyed documents, the Lewy court concluded that certain circumstances might compel the retention of certain records not withstanding the policy. The court reasoned "if the corporation knew or should have known that the documents would become material at some point in the future then such documents should have been preserved." Toward the end, the court concluded, "a corporation can not blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."[97] Thus routine housekeeping dose not necessarily lead to an adverse inference from destruction of evidence. The court in Vick v. Texas Employment Comm'n[98] established the rule that the destruction of documents draws an adverse inference only when they are destroyed in bad faith. Mere negligence is not enough.[99]

The implementation of a reasonable standard seems appropriate as it provides an objective mechanism, which can be assessed by the court. The reasonableness of a particular destruction schedule should however, also be a function of the medium upon which the document exists.[100]

4.3.2. Establishing a retention program

The best way to avoid any inference that the documents were destroyed to avoid litigation is to establish a document retention program.[101] Consider the wide spread use of electronic –based instruments, and the arising potentiality of the damaging electronically stored records, corporations may institute document retention programs for electronic data. Such programs effectively managed, can prevent unnecessary disclosure of information and ensure that documents, which should exist, are available for discovery.[102]

The reasonableness standard for document retention programs suggested by Lewy should apply to document retention program for electronic data. The Lewy court outlined a fair, systematic approach to the review of any particu-

97 Id.
98 514 F.2d 734 (5th cir.1975)
99 Id.
100 Bossiness laws Inc., Guide to Records Retention 112 (1998)
101 "A document retention program involves the systematic review, retention and destruction of documents received or created in the course of business." See, generally Daniel S. Hapke, Jr., Developing and Implementing Records Retention Programs in Business Organizations, in American Corporate Counsel Association, Records Retention Manual (1st ed.Supp.1995) (discussing a " Model Records Retention Guideline")
102 Patrik Grady, Discovery of Computer stored Documents and Computer Based Litigation Support Systems: Why Give up More Than Necessary, 14 J. Marchall J. Computer &Info. L.523, 541 (1996) (discussing considerations to take into account when formulating a record retention program for computerized data.)

lar document retention program.[103] Specifically, the court required an assessment of the "facts and circumstances surrounding the relevant documents".[104] Accordingly, considering the relatively much larger storage capacity of an electronic device when comparing with their paper counterparts, the portion of the reasonableness which once weighed in favour of the corporation's destruction of documents is counterbalanced by society's interest in the retention of records that are reasonably likely to be relevant in current or future litigation. Therefore the retention periods for certain potentially important electronic records should be longer than the retention periods for paper records.[105]

In general, any proper document retention program should be conducted pursuant to a standard policy developed for business reasons that follow specific guidelines such as:

- Potentially important documents should be kept as long as necessary according to the requirement of the law, while the obsolete document should be destroyed systematically;
- Documents relevant to foreseeable or ongoing litigations, investigations etc, are filed systematically and accessible and identified;
- Documents that need to be preserved permanently are catalogued and reduced to forms that are easily stored and retrieved.
- The retention program has regular audits to come in and search files;
- The retention program is organized economically, and dose not bother the business;
- The retention program contains mechanism to stop destruction when necessary.[106]

Usually these general guidelines are not enough. It is advisable for an organization to have some specific plan that targets its electronic storage. Plans including:

103 Id.

104 Supra note 59

105 Corporations should carefully consider the nature of the guidelines outlined in a document retention program for electronic stored data given the array of sanctions that might be imposed following the implementation of an "unreasonable" document retention program. Cf. further Procter& Gamble Co. v. Haugen, 179 F.R.D.622 (D. Utah 1998) (imposing monetary sanctions where a party failed to search a preserve e-mail communications by people with relevant information).

106 See W.F. Reinke, Limiting the Scope of discovery: The use of Protective Orders and Document Retention programs in Patent Litigation, 2 ALB. L. J. SCI & Tech.175

- To have a profile of the company's computer system is necessary to review the hardware and software in use, the inventory of the stored electronic data, and their locations etc;
- Develop policies and procedures regarding creation and retention of electronic information, particularly including e-mail;
- Warn employees to be careful about forwarding messages to other employees and outsiders;[107]
- Instruct employees to encrypt e-mail messages of a confidential or sensitive nature.[108]

Furthermore, computer technology tools are indispensable. A secure computerised system using effective litigation support software with backup routines to keep important document and clear up the irrelevant ones, which helps to create systematic databases and filtering out relevant information using information retrieval techniques etc., will be cost effective for a good document retention program.

5. Conclusion

5.1. Summary

This paper has attempted to explore the issues surrounding the electronic discovery. Given the present dependence upon computers, it is important to realise that the information stored in an organization's electronic media, may become the target of discovery requests. Through the implementation of proactive measures such as those discussed in this paper, an organization should be able to enhance security of its information system, realise more effective management through the use of computer technology, and avoid adverse inference of preserving, destructing, and presenting electronic information in the litigation. Appropriate planning can avoid obsolescence and at the same time it is also important to maintain the integrity and efficiency of the organization's computer system.

Electronic discovery has the potential to reduce costs and shorten the length of civil litigation, although it is widely viewed as costly, time consuming and more complicated than conventional discovery. Most observers believe that in

107 Kenneth Shear, Don't Ignore Electronic Evidence, Tex law, Aug.8, 1994,at 16

108 Judy Temes, E-mail's Dark Side, CFO: The Magazine for Senior Financial Executives Mar.1993, at 13

spite of the cost of electronic discovery, it will eventually overtake conventional discovery, as more and more information is routinely generated, transmitted and stored on computers. Many of the costs associated with computer-based discovery are avoidable through proper management of discovery process, particularly early identification of potential problems and their solutions.

5.2. Suggestions for proper management

At the beginning of this paper, we have explored some unique problems associated with electronic discovery, in the following sections we will indicate some solutions of them based on the research of this paper:

- To preserve the data appropriately it is important for the attorneys on both sides to inform their clients of the duty to preserve potential evidence. Counsel who may be seeking discovery of computer-based information should immediately notify opposing counsel as clearly as possible and may also discuss the bearing of costs.[109] Security measures should also be taken to ensure the confidentiality and integrity of the data.
- The combination of volume and multiple locations may become a headache for the attorneys.[110] Failing to investigate their client's information management system thoroughly may cause adverse inference in court. It is the attorney's obligation to investigate the potentially relevant and discoverable material no matter how technically opaque the system appears. In order to retrieve material efficiently, one may create an electronic information database indexing existing electronic media and details the file sets and directory structure contained in those media.
- The management of large volumes e-mail may need computer search techniques to roughly identify messages. But the result of this may be far from precise. To facilitate discovery, the parties may negotiate an agreement to limit the exposure to each other and to a possible third party. In addition to a retention program, one should exercise some restraint in using e-mail as we mentioned in Section 4, as well as using some litigation support software, which has good function of managing the e-mails.

109 Remarks of Judge Paul Neimeyer on the judicial conference discussion, Draft Minutes of the Civil Rules Advisory Committee, 14-15 Oct 2000,Edward H. Cooper, reporter (on file with the author).

110 Linnen v. A.H. Robins Co., the defendant faced sanctions in the form of costs and a spoliation inference stemming from counsel's failure to completely investigate stored computer back up tapes, while representing to the court that all relevant computer files had been produced.

- It is a relatively simple task for a computer expert or some kind of software to restore routinely deleted data, but it is expensive and the results are uncertain. Before the Rule 16 Pre-trial conference, the attorneys should try to agree on whether restoration of deleted data is expected, to what extent restoration will be required and who will bear the costs.
- Although the discovery of backup is within the scope of the discovery rules, it had the potential to increase the volume of the discovery. It is advisable to reach an agreement between attorneys concerning whether the backup data is needed, to what extent it will be required and the bearing of cost. In addition, using computer software to delete the obsolete data periodically will minimise the volume of back ups, and accordingly save the cost of persevering and retrieval.
- Legacy data is easily ignored. Attorneys should conduct a thorough survey of their client's electronic archives and so called "legacy data" in outdated formats or on outmoded media. A realistic judge should be made for its likelihood of become useful discovery, and balance this towards the cost.

Beyond these solutions we recommended for specific problems. Developing effective electronic discovery management generally needs a document review, retention and destruction policy, as well as a program which include procedures for written communication protocols, data security, employee electronic data storage etc. Clear document policy with the legal awareness as well as the proper use of IT technology will be the basic method for the early effective management of electronic discovery.

Bibliography

I. Cases:

Anti-Monoply v. Hasbro WL 22976 (S.D.N.Y.1996)

Armstrong v. Executive Office of the President, Office of Admin.1 F.3d 1274,1287 (D.C. Cir 1993)

*Bills v. Kennecott Corp*108 F.R.D.459, 461 (D. Utah 1985)

Capellupo v. FMC Corp., 126 F.R.D.262, 265-67 (W.D.La.1982)

Dunn v. Midwestern Indemnity Co., 88 F.R.D.191 (S. D: Ohio 1980)

Fautek v. Montogomery Ward & co., 96 F.R.D.141 (N. D: III 1982)

*Fennell v. First Step Design*83 F.3d 526 (1st cir.1996)

GFTM, Inc. et al. v Wal-Mart Stores, Inc., 2000 WL 335558(S.D.N.Y.)

Kozlowski v. Sears, Roebuck& Co108 F.R.D.459, 461 (D. Utah 1985)

Lewy v. Reminto Arms Co836 F.2d 1104 (8th Cir.1998);

Linnen v. A. H. Robins Co., 1999 WL 462015 (Mass. Super. Ct.),

Peter v. Lacouture, R.I. B.J.9, 11, (Dec.1996)

Procter & Gamble Co. v. haugen, 179 F.R.D.622 (D. Utah 1998)

United States v. Microsoft Corp., Civil action 98-1232(TPJ) (D.C.D.C.12 November 1999)

vick v. Texas Employment Comm'n 514 F.2d 734 (5th cir.1975)

II. Articles and Books

Armstrong, Del and Simonson, John: "Password Guessing" and "Password sniffing", An Intro to Computer Security, School of Engineering & Applied Sciences, University of Rochester, Oct.25, 1996. available at http://www.seas.rochester.edu:8080/CNG/docs/Security/security.html (last visited May 3,2003)

Charles A. Lovell & roger W.Holmes, The Dangers of E-mail: The Need for Electronic Data Retention Policies, 44 R.I.B.J.7, 9 (1995)

Cecilia Magnusson Sjöberg, Electronic Signatures-Measures Required Despite a New Law, *Development and Management of Information Systems in a Legal Perspective*, Stockholm 2001 at 771

Chet Hosmer, President& CEO WetStone Technologies, Inc. Proving the Integrity of Digital Evidence With Time available at http://www.ijde.org/archives/chet_article.html (last visited May 5, 2003)

Cleverdon, C.W. Optimising Convenient Online Access to Bibliographic Database, in Information Services and Use, Vol.4 (1984) nr.1/2 (April) p.37-47

Clonley & Hodge Associates, Manual for Pre-Discovery Disclosure (1994),

Complex Litigation, 11 REV: LITIG.501, 519 (summer, 1992)

Daniel F. Perez, Exploitation and Enforcement of Intellectual Property Rights, 10 Computer Law, Aug.1993, at12

Daniel S. Hapke, Jr., Developing and Implementing Records Retention Programs in Business Organizations, *Records Retention Manual,* American Corporate Counsel Association, 1st ed.Supp.1995.

Delaware State Bar Association, Tips on Technology, www.blankrome.com/publications/articles/ (last visited May 5 2003)

Doblespeak, *Electronic Evidence Discovery*, 2003

Donald C. Massey, Discovery of Electronic Data From Motor Carriers-Is Resistance Futile? *Gonzaga Law Review,* VOL 35:2,at 146-174;

Fred Misko, Jr. Charles E. Ames, Using Technology in the Management and Trial of Complex Cases, *Computer Law Review and Technology Journal,* 1997

Grefory S. Johnson, A Practitioner's Overview of Digital Discovery, 33 Gonz. L.R.347, 360 (1998)

Jacob P. Hart& Anna Marie Plium, Your Opponent's Electronic Media: Some "Disk-Covery" Disputes for the 21st Century, SD43 ALI-ABA 1,Jan.1999, at4; SE63 ALI-ABA, Dec.1999, at 440

James H.A. Pooley & David M. Shaw, Finding Out What's Out There: Technical and Legal Aspects of Discovery, 4 Tex INTELL. PROP. L.J.57, 59 (1995)

John T. Soma& Steven G. Austin, a Practical Guide to Discovering Computerized Files in

Daniel s.hapke,jr., Developing and Implementing records Retention programs in Business Organizations, *American Corporate Counsel Association, Records Retention Manual* 1995

J. Roger Tamer, Preparing for Electronic Discovery, N.Y.L.J., 25 January 1999,at S5

Judy Temes, E-mail's Dark Side, *CFO: The Magazine for Senior Financial Executives* Mar.1993, at 13

Karlgren, Jussi, The Basics of Information Retrieval, Statistics and Linguistics, *Development and Management of Information Systems in a Legal Perspective*, Stockholm 2001 at 208

Kenneth J. Withers, Is Digital Different? Electronic Disclosure and Discovery in Civil Litigation" available at: http://www.kenwithers.com/articles (Last visited April 25,2003)

Kenneth Shear, Esq. "Delete" Doesn't Mean Delete (Revisited) Computer Forensics SANSCA, 1991&1996,last visited April 18, 2003, available at http://rr.sans.org/authentic/improve.php (last visited April 25,2003)

Kenneth Shear, Don't Ignore Electronic Evidence, Tex law, Aug.8, 1994,at 16

Law Computing available at http://www.lawofficecomputing.com (last visited May 9, 2003)

Clonley & Hodge Associates, Manual for Pre-Discovery Disclosure (1994)

Lawrence Argon, E-mail is Not Beyond Law, PC week, 6 October 1997 at 111

Leslie Helm, E-mails Show gates, Others Plotting to Thwart OS Rivals Courts: Cldera offers dramatic evidence to back its claims in a private antitrust action against Microsoft. L.A.Times, Apr.29, 1999, at C1

Lotus Discovery Sever 2.0.1 at

http://www10.lotus.com/ldd/today.nsf/0/3c06ffb3253066b085256cbd0045cdce?OpenDocument (last visited June 20,2003)

Lotus Discovery Sever 2.0 at

http://www10.lotus.com/ldd/today.nsf/9148b29c86ffdcd385256658007aaa0f/ea27b7f8979c99ac85256b9d00030b29?OpenDocument (last visited June 20,2003)

Luuk Matthijssen, Interfacing Between Lawyers and Computers, at 19-30,Katholieke Universty, 2000

MacGregor, Tina: Password Auditing and Password Filtering to Improve Network Security, SANSCA, 1991&1996, available at http://rr.sans.org/authentic/improve.php (last visited April 18, 2003),

Maria Gold, He-said, She-said Divorces Take on Twist With E-mail, Boston GLOBE, 2 May 1999,at A 16

Mark D. Robin, Computers and the Discovery of Evidence: a New Dimension to Civil Procedure, 17 J, Marshall J. of computer and info. L.411, 419 (1999)

Matthew Goldstein, Electronic Mail, Computer Message Present Knotty Issues of Discovery.N.Y.L.J.,Feb.8,1994,at1

Michael R. Overly, Source of Electronic Evidence, *Electronic Evidence in California* (1999) 2-31

Paul F. Enzinna, An E-mail Top Teten: 5 Reasons To Worry, and 5 Ways To sleep At Night, The Practical Litigator, July 1999,at 47, 48

Patrik Grady, Discovery of Computer stored Documents and Computer Based Litigation Support systems: Why give up More than Necessary, 14 J. Marchall J. *computer &Info*. L.523, 541 (1996)

Ron Chepesiuk, Trial by E-mail, STUDENT LAW, Sep.1998, at 31,31-32

Russell, Deborach and Gangemi Sr., G.T.: Computer Security Basics, O'Reilly &Associates, Inc.Sebastopol, CA, 1991.

Samuel A. Thumma, Electronic Mail in the Workplace: Litigation Trends for 1998 (visited April 22,2003) http://www.brownbain.com

Tuomas Poysti, Information Security Commentary, available at http://www.uroa.fi/home/oiffi/enlist/commentary/information_security.html , Context Ltd.,2000 (last visited Jan 9,2002)

University of Michigan, Information Technology Division, and Password Security: A Guide for Students, Faculty, and Staff of the University of Michigan, Reference R1192, and Revised April 1997. http://www.umich.edu/~polices/pw-security.html (last visited May 5,2003)

Virignia Lewellyn, Discovery the E-way, available at http://www.law.com/jsp/printerfriendly.jsp?C=LawArticle&t=PrinterF.(last visited May 5 2003);

W.F. Reinke, Limiting the Scope of discovery: The Use of Protective Orders and Document Retention Programs in Patent Litigation, 2 ALB. L. J. SCI & Tech.175

10 ARTICLE 11 OF THE ELECTRONIC COMMERCE DIRECTIVE: A FAILED ATTEMPT TO HARMONISE ELECTRONIC CONTRACT FORMATION?

Maryke Silalahi Nuth[1]

The law of contract has a long history. Throughout centuries, the law of contract has evolved into the structure that we have today and the significance of the contract has changed within the legal psyche of lawyers since it emerged as a subject in its own right.[2] In this electronic age of instantaneous communications, the growth of information technology has facilitated the use of contracts. Many contracts are daily entered into in the online environment. As the use of World Wide Web to display advertising and promotional materials become more common, the number of contracts concluded on the Internet is also increasing.

Apart from financing commercial communication, online transactions (contractual undertakings, online payments, subscriptions) are significant sources of revenue on the Internet. The ability to form enforceable contracts online is a fundamental requirement to the growth of electronic commerce on the Internet. For the European Union (EU), the widespread use of e-commerce in the financial service sector will enhance the functioning of the EU internal market. Thus, the EU has the interest to ensure that the online contract is enforceable, and simultaneously that consumers are confident about the contractual arrangement that apply to their transactions. This has led to the adoption of the European Union Directive on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("E-Commerce Directive").[3] Section 3 of this directive covers regulation concerning electronic contracts as provided in its articles 9-11. These articles aim to remove the restrictions on the enforceability of electronic contracts due to their electronic nature (article 9), to ensure that the recipient of services is pro-

1 The author is doctoral research fellow at the Norwegian Research Center for Computers and Laws, University of Oslo.

2 Paul Richards, Law of Contract, 5th Edition, Pearson Education Limited, 2002, p. 5.

3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, O.J. L178, 17.7.2000.

vided with explanatory information when entering into an electronic contract (article 10) and to impose obligations on the service provider in relation to the placing of order by the recipient of the services (article 11).

As the first attempt in the EU level to harmonise the general rules on electronic contract formation, article 11 of the E-Commerce Directive invites controversies. The final text of this article raises questions both of interpretation and implementation. Some of the EU Member States concluded that this article has no effect in the contract formation and thus general contract rules on the formation of contract will continue to apply. This article will explore if there are justifications that support this opinion and whether article 11 of the E-Commerce Directive achieves its purpose to harmonise the electronic contract formation in the EU.

1. Roads to adoption

The initial draft of article 11 of the E-Commerce Directive contained detailed private law regulations on how electronic contracts were to be formed and when a contract is concluded electronically.[4] In the first draft, the EU Commission attempted to harmonize the time at which a contract is concluded. The EU Commission proposed that an electronic contract, where a recipient is required to give his consent through technological means, is deemed to be concluded when the recipient of the service has confirmed receipt of the service provider's acknowledgement of receipt of the recipient's acceptance. This means that a contract's recipient is required to restate his or her desire to conclude such contract. In a more clear term, four steps were required for a contract to be concluded online:

1. An offer is made by the website.
2. By filling out a form and clicking on 'OK' to the purchase, the contract is accepted.
3. An automatic email sent by the service provider's system provides the acknowledgement.
4. The recipient must reply to such acknowledgment and the contract will be considered concluded when the service provider has been able to access such reply.

This draft article addressed the fundamental requirements in determining when a contract is concluded electronically. The mechanism of concluding a

4 COM (98)586 OJ 1999 C30/4.

contract specified in this article goes further than required by the traditional concept of contract formation whereby the mere exchange of `offer and acceptance' is enough to bring about a contract. By requiring the service provider to provide acknowledgment of the recipient's acceptance and the recipient to reply to such acknowledgement before a contract can be concluded, this draft article adds two steps in the formation of electronic contract that is not usually required in the formation of non-electronic contract.

The above proposition was simplified by the EU Parliament's 42nd amendment to the proposal which stipulated: when a recipient is required to give his consent through technological means, a contract will be considered concluded when the service provider has acknowledged the receipt of the recipient's acceptance. Here it is no longer required for the recipient of the service to reply to the acknowledgement of acceptance sent by the service provider. In other words, the procedure of electronic contract formation is reduced into three-step formation procedure:

1. An offer is made by the website.
2. By filling out a form and clicking on 'OK' to the purchase, the contract is accepted.
3. An automatic email sent by the service provider's system provides the acknowledgement and only when the recipient has been able to access such acknowledgement would the contract be considered concluded.

This new simplified draft was designed to specifically address the following situations:

- a concrete offer made by a service provider (and thus the situation in which the service provider only issues an invitation to treat is not covered);
- a contractual process in which the recipient of the service only has the choice of clicking "yes" or "no" (or the use of other technology) to accept or refuse an offer;[5]
- an acknowledgement of acceptance is provided by the service provider in form of automatic email (and thus the situation in which the acknowledgement of acceptance provided by other technology is not covered).

5 The European Commission, A proposal presented for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market - Commentary on individual articles, January 1999, p. 9.

Only little of the proposed harmonisation and its amendments did eventually remain in the final version of article 11(1) of the E-Commerce Directive. Instead of using a three-step-formation-procedure, the adopted article 11(1) of the E-Commerce Directive suggests the use of a two-step-procedure:

1. The service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.
2. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

As opposed to the initial draft, this final version of the article gives no clarification as to the status of a website, whether it amounts to an offer or an invitation to treat. To some extent this may be seen as an advantage because by not limiting its application to a specific type of website, this article can be applied to all websites regardless their status as an offer or an invitation to treat. Previous proposals covered only the situation where a website constitutes an offer and left website constituting invitation to treat with no clear regulations. Nevertheless the fact that the E-Commerce Directive does not define – implicitly or expressly – that a website constitutes an offer or invitation to treat may have some consequences. Treating the website as invitation to treat will lead to a situation where the service provider retains freedom to contract. By clicking an "OK" button, the customer offers to buy the goods/services. This offer has no binding power on the service provider until he accepts it. He can avoid entering into contract with online buyers and refuse the customer's offer without having to explain why he is refusing the offer. This may raise the concern of consumer protection in B2C (Business-to-Consumer) transactions. On the other hand, when an offer is considered to be made by the website, it is binding on the service provider. Once the customer clicks on the "OK" button – which may be considered as an acceptance – the contract is concluded and the service provider can not avoid the contract.

In spite of the foregoing, it should be noted that different national laws and regulations in EU Member States may bring different solutions to the abovementioned situations.

2. Stumbling blocks in electronic contract formation?

Article 11 of the E-Commerce Directive makes reference to some terms or concepts to be used in the process of electronic contract formation such as "acknowledgement of receipt", "order" and "able to access".

2.1 Acceptance and acknowledgement of receipt of order

In practice, it is important to know whether the offeree's reply to an offer is merely an acknowledgement of receipt or is in fact an acceptance of an offer. This will clarify whether the offeree intended to be bound or was only telling the offeror of receipt of the offer. In the first alternative the offeree was bound by a contract which was concluded by his reply, while in the second he remained free to reject the offer. Such uncertainty generally arises where the language of the statement is ambiguous or not clear and thus interpretation is needed.

Article 11(1) of the E-Commerce Directive requires the service provider to acknowledge receipt of the recipient's order but did not define the meaning or the effect of the acknowledgement of receipt of order. Therefore a look at the practice may perhaps help to clarify the meaning of this term. However, it is not always easy in practice to determine the status of an acknowledgement. Very often documents titled acknowledgement of receipt or confirmation only contain a repetition of the terms that the parties are already bound to or details parties' order. This is commonly found especially in the Internet situation. The usage of automatic mailing enables the service provider to automatically send an acknowledgement of receipt of the customer's order.[6] Some websites even provide automatic display of acknowledgement of receipt of the order in the website directly after the customer clicks on the 'OK' or 'submit' button. The acknowledgement of receipt provided with the above mentioned mechanism will usually only contain a repetition of the terms of the order and thus serves as a confirmation on the receipt of the order. On the other hand, an acknowledgement of receipt can also be construed as acceptance to the order. This usually occurs when an acknowledgement of receipt of order does not merely repeat the terms of the offer but also contains some other words that may be construed as indicating an acceptance to the offer.

From the foregoing, there are two possible ways of interpreting the acknowledgement of receipt of order stipulated by article 11 of the E-Commerce Directive. If such acknowledgement of receipt is construed as a mere confirmation of the customer's order, it basically has no legal effect other than proofing that the order has been placed. A confirmation is not a required element to bring about a contract. Consequently, the lack of acknowledgement or confirmation has no legal effect in contract formation. On the other hand, if acknowledgement of receipt of order under article 11 of the E-Commerce Directive constitutes an acceptance, this article is basically only restating gene-

6 The customer will receive such acknowledgement of receipt in his email box provided that he supplies the website with correct email address.

ral rules of contract formation that an acceptance (as contained in acknowledgement of receipt) needs to be communicated and effective when the addressee is able to access it. Leaving the notion of "able to access" for later discussion, by only restating general rules of contract formation it is doubtful if a harmonisation of electronic contract formation can be achieved. Nevertheless it is logical to suggest that the requirement to provide acknowledgement of receipt is aimed to give more security and certainty for the customers – so that they will know what they have ordered and the terms of the order.

2.2 Order

Article 11 of the E-Commerce Directive uses the term "order" which makes this article even more confusing. 'Order' is not a common concept used in the legislation on formation of contracts.[7] In the Internet situation, the term 'order' can be interpreted differently depending on the status of the website. When a website amounts to an invitation to treat, an order from the customer will be an *offer* to purchase the goods/services. On the other hand, when a website constitutes an offer to customers, an order placed by the customer will constitute an *acceptance*.

The abovementioned interpretations of order, will lead to different results. There is little complexity when an order is deemed to be an offer. The placing of such order in the Internet, does not put any obligation on the website owner to provide the ordered goods/services. However, when an order constitutes an acceptance, the communication of the order places a binding obligation on the website owner to provide customers with the ordered goods/services.

2.3 Able to access

Article 11 of the E-Commerce Directive provides that the order and the acknowledgement of receipt are deemed to be received when the recipient is "able to access" them. Although this article provides certainty as to the moment when an order or acknowledgement of receipt is deemed to be received, there is no explanation as to the meaning of "able to access". Therefore "able to access" requires further interpretation by EU member countries which inevitably may lead to different implementations of this notion from one member country to another. Some suggestions on when the message is accessible include: (i) when the message has entered the recipient's network or server, (ii) when the message

7 Christine Hultmark Ramberg, 'The E-Commerce Directive and Formation of Contract in a Comparative Perspective' (2001) Global Jurist Advances, No. 2, p. 15.

is already in the recipient computer system, (iii) when the message is already in the mailbox of the recipient.

It would seem that being `able to access' is such an indeterminate criteria for establishing the conclusion of a contract since either party may use any number of excuses in order to avoid conclusion of a contract, if that is their intention. For example: one party may say that he has not been able to *access* the acknowledgment of receipt of order because his network/server has been down for several days. Of course, there is also possibility that the order or acknowledgement of receipt never reaches the other party or is delayed for other reasons that can be attributed to be within the sender's or the addressee's sphere of control. Here comes the question of which of the parties should bear the risk of a message not reaching the addressee or being delayed. This placement of risk is important especially in an online environment where the time is of the essence.

For comparative purposes, we can look at the provision of the US Uniform Electronic Transaction Act ("UETA") and the UNCITRAL Model Law on Electronic Commerce ("UNCITRAL Model Law"). Both these legal instruments have analysed in depth the general concept of "able to access" by stipulating when messages are considered "received" since it is at this moment the ability to access occurs. The UETA provides that an electronic record is received when (a) it enters the information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record and (b) it is in a form capable of being processed by that system.[8] The UNCITRAL Model Law regulates that receipt of an electronic message occurs (i) at the time when the data message enters the designated information system or (ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee.[9] However, if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.[10] These provisions illustrate that it is possible to provide extensive guidance as to the exact moment when the ability to access or the receipt occurs. Noticeably both UETA and UNCITRAL Model Law provide more helpful guideline on the time of receipt of electronic communication than the EU E-Commerce Directive. However, it should be noted that the rules in the UETA and UNCITRAL Model Law

8 Section 15(b) US Uniform Electronic Transaction Act.
9 Article 15(2)(a) of the UNCITRAL Model Law on Electronic Commerce.
10 Article 15(2)(b) of the UNCITRAL Model Law on Electronic Commerce.

apply to all electronic records as opposed to the rules in article 11 of the E-Commerce Directive which only cover limited type of messages (order and acknowledgement of receipt).

2.4 Correction of input error

Article 11 (2) of the E-Commerce Directive stipulates that the service provider should make available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct errors, prior to the placing of the order. This provision adds a new obligation for service providers which can prove hard to implement. Nowadays it is common to place an order just by clicking on the 'OK' or 'submit' button appearing in the provided form. To avoid or detect the error, a user is usually required to check his input before he clicks on such buttons. There is no special means in place to correct and identify input errors before he places the order. A simple click on the 'OK' button will mean placing the order to the service provider and the customer has no opportunity to correct any error that he may have done before he click on the 'OK' button. This can lead to a situation where the customer is bound to a contract with unwanted terms resulting from input error. As such this method does not seem to be enough to fulfil the requirement of article 11(2) of the E-Commerce Directive.

Under online shopping circumstances where time is of the essence, it would be reasonable to expect that input errors can be corrected in order to identify or correct the terms of the order. The E-Commerce Directive tries to achieve this by requiring the existence of technical means capable of allowing the customer to identify and correct input errors before placing the order. Such technical means will allow the customer to read all the information he has input and identify any error that possibly exist before he actually binds himself to the terms of the order by clicking on 'OK' button that places the order to the website provider. This can be achieved by putting in place a second page or confirmation windows that show the contents of the submitted form and requiring the customer to confirm that input by clicking once again on the 'OK' or similar button. In this second page, the customer should also be able to correct the input if needed. This means the customer must perform double clicks before sending the order. This scenario is purported to protect, and therefore benefit, the customer but not always benefit the service provider. Although double click system can provide certainty to the service provider on the acceptance of his offer or invitation to treat, the building of second page to allow identifying and correcting errors can be very costly. In the end, this requirement can discourage the service provider from taking the advantage

of electronic commerce. One of the reasons for investing in online business is because it would save the investor from investing money in the stores or other facilities. When the cost of conducting business online becomes very high, this will discourage the existing investor or service providers to continue their business online or making further investments.

Alternatively, some service providers may try to send by email an overview of the order and ask the customers whether they really want to order the goods/services. Although appropriate, this may not be the most effective way to conduct business in the Internet. The answer from the recipient may be delayed which is possibly not in the interest of the service provider who usually wants to sell his goods/services quickly. Therefore, a page presenting an overview of what has been ordered and allowing the identification and correction of input errors before sending the order to the service provider as required by the E-Commerce Directive seems to be the most appropriate, effective and accessible way.[11]

The rationale for the requirement of technical means to identify and correct input errors is to properly secure the intention to be bound to an electronic transaction and prevent mistake in the expression. It is often the case in the Internet situation where the "OK" or "send" button is clicked accidentally or too early and there are still some errors in the input data. When this click brings about a contract, the person will be bound to a contract without having any intention to do so. Since online transaction happens in a significant speed and sometimes by the way of automation, this mistake will reach the addressee very shortly after the click and the addressee may take action in reliance of this message. The question will be who should bear the risk of the mistake in expression?

To create an incentive to act carefully and avoid mistake from being communicated, the risk for mistake has traditionally been placed upon the party making a mistake.[12] The relying party is therefore entitled to compensation of the loss incurred in relying on the mistake. This is particularly relevant when there was no mistake but merely a change of mind. However, it is not always easy to know for sure whether a mistake has indeed happened or it is just merely a change of mind.

In the course of e-commerce development, there has been a trend to impose less liability on a party making mistakes in expression (input errors). This trend can be found in UETA Section 10(2) that shifted the burden onto the party relying on the mistake. This provision is purported to create a strong incentive on the service provider to introduce a confirmation page. The confirmation page

11 Arno R. Lodder and Henrik W.K. Kaspersen, eDirectives: Guide to European Union Law on E-commerce, Kluwer Law International, 2002, p. 86.

12 Ramberg, supra note 7, p. 19.

will delay the sending of the data and provide the customer with time to read what they have input and eventually make the necessary corrections. This mechanism will reduce mistakes in online transactions. Where such confirmation procedure is in place, the party making the mistake has to bear the risk.

It had been suggested that the trend of imposing less liability on a party making mistake in expression can also be found in article 11(2) of the E-Commerce Directive. However, this argument may not be entirely true. This article only regulates as far as the requirement to put in place appropriate, effective and accessible technical means to identify or correct errors and does not address the distribution of liability in connection with mistake. This article is silent on who should bear the risk when the service provider has put in place the required technical means but still there is a mistake on which the service provider has relied. Although it is highly possible that the party making mistake is the one who should bear the risk, such rationale is not expressly provided under article 11 of the E-Commerce Directive. The different legal systems of EU Member States may provide different approaches and solutions to such a situation in each country. It is however clear that this article does imply that when the required technical means is not put in place and the service provider relies on the input error of the customers, the service provider will bear the risk.

Article 11 of the E-Commerce Directive does not provide any consequences or sanctions when the required technical means is not provided by the service provider. Article 20 of the E-Commerce Directive stipulates that it is up to the Member States to regulate the sanction on the infringement of the national provisions adopting the E-Commerce Directive including failure to make available technical means as required by article 11(2) of the E-Commerce Directive. This may lead to the inconsistency of the application of this article. EU Member States have different legal systems application of which may lead to different interpretation of the necessity to put in place the required technical means, its legal effect and the sanction on the service provider's inability to provide such technical means.

3. Auxiliary observations

3.1 Application of the Receipt Rule

The general rule of contract formation that acceptance must be communicated to the offeror is also applicable to electronic contract. Online acceptance can be made by the same mode of communication used to make the offer in the first place or by using other more reliable mode. It follows that an offer received by

email may also be accepted by email unless the offer specifies some other mode of acceptance. Similarly, an offer placed through a website shall also be accepted through that website, unless the offer specifies some mode of acceptance or there are other equally expeditious or reliable methods of communication.

An acceptance has no effect until it is communicated to the offeror because it could cause hardship to an offeror if he is bound without knowing that his offer had been accepted.[13] There are many approaches that can be used in deciding when the acceptance is deemed to be effective. The Postal Rule theorists view the acceptance effective when it is sent or dispatched. The Receipt Rule theorists consider the acceptance effective when it is received by the offeror. The Knowledge Rule theorists regard the acceptance as effective when the fact of acceptance comes to knowledge of the offeror. Article 11 of the E-Commerce Directive does not give guidance as to which rule should be applied to the communication of acceptance. This article only covers the communication of order and acknowledgement of receipt of order, both of which deemed to be received (and thus effective) when it is possible to access them. Putting together the notion of "able to access" and the foregoing theories to decide when the order and acknowledgement of receipt is effective leads to three possible situations:

1. *No access*. The Postal Rule is not likely to apply since when the document is sent to the post office and thus comes under the control of the post office, it is not likely that any of the parties has access to it. The intended recipient can only have access to it when the post office actually delivers it to him. Although debatable, this rule may be applicable in online environment by making an analogy between post office and other technological means of delivering messages.
2. *Able to access*. Under the Receipt Rule it is required for the communicated document to reach the intended recipient. When the document reaches the recipient, it is reasonable to presume that the addressee is able to access the document.
3. *Use of access*. The Knowledge Rule requires the actual knowledge of recipient that usually can be acquired by reading the communicated document. To be able to obtain such knowledge or to read the document, the recipient must already have access to the document and make use of such access.

Both number 1 and 3 are not the situations described by the E-Commerce Directive which clearly mentioned that the communicated document is deemed to be received when the intended party is 'able to access' it. The wording

13 G.H. Treitel, The Law of Contract, 11th Edition, Sweet & Maxwell, 2003, p. 23.

'able' in this phrase makes it clear that the party must posses the ability to access without necessarily 'access' the communicated document. Such requirement is fulfilled under the application of the Receipt Rule. Accordingly it is then possible to suggest that E-Commerce Directive prefers the application of the Receipt Rule in the communication of order and acknowledgment of receipt of the order. This situation may bring some difficulties to the EU Member States whose contract laws are in favour of the Postal Rule. The situation will be easier for the countries applying the Knowledge Rule because the minimum requirement for the application of the Knowledge Rule doctrine is that the intended recipient must already have access to the communicated document.[14] This means that for someone to have knowledge of a document, he needs to have had access to it. As such, the ability to access as required by the E-Commerce Directive is already in existence.

3.2 Consumer protection

As article 11 of the E-Commerce Directive requires the service provider to issue an acknowledgement of receipt of the recipient's order, it can be said that this article makes it *compulsory* for the service provider to issue an acknowledgement of receipt of order. This means that even if the customer does not request any confirmation from the service provider of the placed order, the service provider is obliged to provide an acknowledgment of receipt to the customer. It follows that in the event the service provider does not or is unable to provide any acknowledgement of receipt of the order placed by the customer; such service provider is in breach of the provision of article 11 of the E-Commerce Directive. Consequently this article provides certainty and protection to the customer when dealing with service provider as it guarantees the service provider will provide the customer with an acknowledgment of receipt of order even if the customer does not request for it.

The fact that application of article 11 of the E-Commerce Directive is mandatory to the Business-to-Consumer ("B2C") transactions but not for Business-to-Business ("B2B") transactions supports the argument that this article is indeed mainly aimed to protect consumers. But since there is no legal consequence of the lack of acknowledgement under general contract law and the fact that E-Commerce Directive also does not provide any consequence of the lack of the acknowledgement of receipt, this protection may end up becoming insignificant except for evidentiary purpose. This proposition is without

14 It is suggested and agreed by many legal scholars agreed that Knowledge Rule could be seen as a variant of Receipt Rule.

prejudice to the fact that, although highly unlikely, EU Member States may regulate what is the consequence of the failure of service provider to provide an acknowledgement of receipt of order as permitted by article 20 of the E-Commerce Directive.

Concluding remarks

Article 11 of the E-Commerce Directive contains many unclear words leading to uncertainties on the implementation of this article. The attempt to make it mandatory for the service provider to provide acknowledgement of receipt has no effect to the formation of contract. Unclear status of "order" and the lack of clarification of what constitute "able to access" add more uncertainties as to how to implement this article. Furthermore, the fact that this article provides no legal consequences of the failure (i) to conform to the provision that the order and acknowledgement of receipt are deemed to be received when the addressees are "able to access" them, (ii) to provide "appropriate, effective and accessible technical means" to identify or correct input errors, puts the implementation of these provisions at risk.

Despite the above criticism, it should also be mentioned here that article 11 of the E-Commerce Directive provides certainty as to the application of Receipt Rule in the communication of order and acknowledgment of receipt. This article also introduces the double clicks requirement to allow the correction of input errors in early stage of contract formation. Since it is mandatory for the service provider to fulfil the requirements provided under this article in the B2C transaction but not when contracting in the B2B relationship, it is clear this article purported to provide certainty and protection especially to consumers in electronic transactions. This will hopefully increase the confidence in electronic transaction and encourage more people to conduct online transactions, which in turn will benefit the EU internal market.

11 POLITI, PIRATERI OG KODEKNEKKING[1]

Inger Marie Sunde

1. Endringer i straffeloven og åndsverkloven

Jurister med interesse for spørsmål knyttet til pirateri og kodeknekking, har spennende tider. Delvis foranlediget av tiltredelsen til Cybercrime-konvensjonen,[2] og delvis som følge av gjennomføringen av opphavsrettsdirektivet,[3] er det blitt vedtatt flere nye bestemmelser som berører slike spørsmål.

Cybercrime-konvensjonen pålegger konvensjonspartene å sørge for at den nasjonale straffe-, og prosesslovgivningen oppfyller visse minimumskrav. Konvensjonsbestemmelsene i art. 2-6 og 10 gjelder straffbare handlinger rettet mot datasikkerheten og opphavsrettskrenkelser, og danner et bakteppe for problemstillingene som drøftes i denne artikkelen. Ot.prp. nr. 40 (2004-2005) omhandler de tilpasninger som er nødvendige for å ratifisere Cybercrime-konvensjonen, og bygger videre på utredningen til Datakrimutvalget avgitt i NOU 2003: 27 Lovtiltak mot datakriminalitet. Stortinget behandlet proposisjonen våren 2005 og vedtok blant annet en endring i straffeloven § 145 annet ledd og føyde til en ny bestemmelse i strl. § 145b.[4] Lovendringene trådte i kraft med umiddelbar virkning.

Strl. § 145b lyder *"den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler"*. Ved straffskjerpende omstendigheter øker strafferammen til fengsel inntil 2 år, jf. annet ledd. Som eksempler på slike omstendigheter nevnes *"om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen forøvrig skaper fare for betydelig skade"*. Av tredje ledd fremgår det at medvirkning er straffbart. Skyldkravet er forsett, jf. strl. § 40.

---

1 Denne artikkelen er en bearbeidet versjon av artikkelen "Politi, pirateri og kodeknekking" publisert i Tidsskrift for Strafferett 2005 nr. 2. Bearbeidelsen ledet til at jeg har endret noen av de standpunkter jeg tidligere inntok. Dessuten er enkelte tema nå noe mer utdypet.

2 Europarådets konvensjon vedtatt 8. november 2001 (185 ETS), undertegnet av Norge 23. november samme år. Pr. oktober 2005 har 32 stater undertegnet og 5 ratifisert konvensjonen.

3 Direktiv 2001/29/EF av 22. mai 200.

4 Jf. endringslov av 8. april 2005 nr. 16. Se Innst.O. nr. 53 (2004-2005), og Besl.O. nr. 48 (2004-2005).

Strl. § 145b, slik den ble vedtatt, er utformet i samsvar med minimumskravet i Cybercrime-konvensjonen art. 6 pkt. 1.a.(ii), jf. pkt. 3. Justiskomitéen gikk kortere enn departementet, som i tråd med anbefalingen i art. 6, både hadde foreslått å straffbelegge flere befatningsformer enn spredning, og at slik befatning skulle være straffbar ikke bare med hensyn til tilgangskoder, men også for *dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer.* Formuleringen tok sikte på å ramme befatning med hackerverktøy og skadelig kode, som f. eks. datavirus.[5] Bortsett fra spredning, var bestemmelsen foreslått også å ramme *fremstilling, anskaffelse og besittelse*. Forutsetningen var at befatningen var rettsstridig, jf. vilkåret *"uberettiget"*. Justiskomitéen uttalte at den så det *"prinsipielle i problematikken rundt det å kriminalisere forberedelseshandlinger og det å være i besittelse av datavirus, hackerverktøy og lignende"*. Komitéens mindretall la imidlertid størst vekt på at *"de typer innretninger det er tale om har et begrenset lovlig bruksområde og kan brukes til å begå alvorlige straffbare handlinger"*, og støttet derfor regjeringens lovforslag. Flertallet derimot, gikk inn for minimumsløsningen, jf. lovsitatet ovenfor, noe som ledet til at Norge måtte benytte seg av reservasjonsadgangen etter art. 6 nr. 3.[6]

Justiskomitéen foretok også en endring i "datainnbruddsbestemmelsen" i strl. § 145 annet ledd. Tidligere inneholdt straffebudet et vilkår om *"å bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data"*. Dette beskyttelsesbruddvilkåret ble fjernet. Etter lovendringen er det tilstrekkelig for overtredelse at man *"uberettiget skaffer seg adgang til data"*. Denne endringen var verken påkrevet etter Cybercrime-konvensjonen eller foreslått av departementet. Departementet hadde riktignok vurdert behovet for et økt vern om data ved å fjerne beskyttelsesvilkåret, men mente at en slik endring burde vurderes i en bredere sammenheng av Datakrimutvalget i dets videre arbeid.[7] Justiskomiteen mente imidlertid at behovet for endring var mer akutt og fjernet beskyttelsesvilkåret.

Med denne lovendringen tok Stortinget et langt steg vekk fra det syn som straffebestemmelsen har hvilt på siden revisjonen av datavernbestemmelsene i 1987.[8] Revisjonen bygget vesentlig på Straffelovrådets utredning av 1985, hvor man blant annet skrev at *"bruken av sikkerhetsforanstaltninger har [utvilsomt] en langt større preventiv betydning enn den nærmere utforming av straffebestemmelsene. Hensiktsmessige straffebestemmelser kan aldri tre i*

5 Ot.prp. nr. 40 (2004-2005) s. 17 flg., pkt. 3.3.4.3.

6 Innst.O. nr. 53 (2004-2005). Se Justiskomiteens merknader i pkt. 2.

7 Se Ot.prp. nr. 40 (2004-2005) s. 14-15, pkt. 3.2.6.

8 Jf. endringslov av 12. juni 1987 nr. 54.

stedet for innehavernes egen virksomhet for å beskytte dataanlegget". Videre står det at *"det primært hviler på innehaveren av anlegget å sørge for beskyttelse mot innsyn fra uberettigede. Først når det er tatt rimelige foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet"*.[9]

Som følge av krav i opphavsrettsdirektivet ble åndsverkloven endret ved endringslov av 17. juni 2005 nr. 97. Av spesiell interesse i vår sammenheng er åvl. § 53a, som gjelder forbud mot omgåelse mv., av effektive tekniske beskyttelsessystemer. Den delen av bestemmelsen som direkte gjelder beskyttelsesbrudd står i første ledd og lyder *"[d]et er forbudt å omgå effektive tekniske beskyttelsessystemer som rettighetshaver eller den han har gitt samtykke benytter for å kontrollere eksemplarfremstilling eller tilgjengeliggjøring for allmennheten av et vernet verk"*. Bestemmelsen må leses i sammenheng med presiseringen av eneretten i åvl. § 2, se tredje ledd bokstav c, jf. fjerde ledd, som lyder: *"Verket gjøres tilgjengelig for allmennheten når verket fremføres offentlig. Som offentlig fremføring regnes også kringkasting eller annen overføring i tråd eller trådløst til allmennheten, herunder når verket stilles til rådighet på en slik måte at den enkelte selv kan velge tid og sted for tilgang til verket"*. Det presiseres altså at kringkastingssendinger og verk som overføres online som såkalte on demand-tjenester, omfattes av eneretten til fremføring for allmennheten. Omgåelse - eller krenkelse - av tekniske beskyttelsessystemer som verner slike tjenester, rammes av åvl. § 53a første ledd, etter det alternativet som gjelder *"å kontrollere... tilgjengeliggjøring for allmennheten av et vernet verk"*. Etter bestemmelsens annet ledd oppstilles et forbud mot forskjellige former for befatning med omgåelsesverktøy og -tjenester, jf. oppregningen i bokstav a-e. Bestemmelsens tredje ledd inneholder visse unntak fra forbudene i første og annet ledd, herunder unntak for *"forskning i kryptologi"* og for *"privat brukers tilegnelse av lovlig anskaffet verk på det som i alminnelighet oppfattes som relevant avspillingsutstyr"*. Bestemmelsen er straffesanksjonert, jf. åvl. § 54 første ledd bokstav b. Straffansvaret omfatter forsettlig og uaktsom overtredelse, samt medvirkning. Strafferammen er bøter eller fengsel inntil tre måneder. Ved forsettlig overtredelse under særlig skjerpende forhold øker strafferammen til bøter eller fengsel inntil tre år, jf. åvl. § 54 fjerde ledd.

2. Om eksisterende bestemmelser - og linjen frem til åvl. § 53a

Det er interessant å se på utviklingen bak reglene, som alle har med uberettiget tilgang til data å gjøre. Den nylig endrede «datainnbruddsregelen» i strl. § 145 annet ledd, er en videreføring av en datavernbestemmelse opprinnelig inntatt i

9 NOU 10985: 31 Datakriminalitet, s. 30. sp. 2 nederst og s. 31 sp. 2.

strl. § 145 første ledd annet punkt, i 1979.[10] Etter Straffelovrådets utredning i 1985,[11] ble regelen i 1987 skilt ut til et nytt annet ledd i § 145, samtidig som gjerningsbeskrivelsen ble noe omformulert.[12] Mens det etter lovendringen i 1979 var tilstrekkelig at meddelelsen eller opptegnelsen var *"lukket"*, ble det i 1987 oppstilt krav om beskyttelsesbrudd eller omgåelse av en beskyttelse. Ubeskyttede data hadde således ikke vern etter bestemmelsen, selv om gjerningspersonen skulle være klart uberettiget til dem. Det vises til Straffelovrådets begrunnelse sitert i kapittel 1. I så fall måtte andre bestemmelser anvendes, f. eks. reglene om ulovlig bruk av løsøregjenstand, jf. strl. § 261 og § 393, reglene om ulovlig innsyn i eller bruk av hemmeligheter, jf. strl. §§ 90-91 (rikets sikkerhet), strl. § 294 nr. 2 og 3, § 405a og markedsføringsloven[13] § 7, jf. § 17 (forretnings- eller bedriftshemmeligheter), eventuelt reglene om økonomisk utroskap i strl. § 275 flg., og endelig, åndsverklovens regler til vern om opphavsrettigheter og nærstående rettigheter.[14] Ved endringsloven av 8. april 2005 nr. 16, har imidlertid ubeskyttede data fått et generelt strafferettslig vern etter strl. § 145 annet ledd. Det er heller ikke noe krav om at dataene er "lukket".

Oslo tingrett avsa fellende dom den 10. mars i år, i en sak som illustrerer kombinasjonen av straffebestemmelser ved "datatyveri".[15] Domfelte var en 39 år gammel mann i ledelsen i et telemarketingselskap (fornærmede) med 500 ansatte. Etter at han hadde innledet forhandlinger om ansettelse som administrerende direktør i et konkurrerende selskap, tilegnet han seg alt innhold på fornærmedes "produksjonsserver". Han kopierte totalt 23 000 datafiler til 5-7 CDer, som han tok ut av bedriften. Innholdet besto av elektroniske dokumenter relatert til fornærmedes virksomhet, herunder bedriftshemmeligheter som informasjon om kunder og rapporter om økonomi- og fortjenesteforhold i bedriften. I tillegg tok han med seg et anbud utarbeidet av fornærmede til et prosjekt verdt ca. kr 200 millioner, ved å sende anbudet til sin private frisurf e-postkonto. Samme dag undertegnet han ansettelsesavtale med konkurrenten om stilling som administrerende direktør, og sa opp sin stilling hos fornærmede.

---

10 Jf. endringslov av 16. februar 1979 nr. 3.

11 NOU 1985: 31 Datakriminalitet.

12 Jf. endringslov av 12. juni 1987 nr. 54.

13 Lov 47/1972.

14 Også tyveri- og underslagsbestemmelsene er aktuelle, men i teorien har man vært avvisende til anvendeligheten på data, på grunn av vilkåret "gjenstand". Dette forstås som et krav om fysisk beskaffenhet. Det er grunn til å stille seg kritisk til denne lovforståelsen, som heller ikke er blitt satt på spissen for Høyesterett. Det kan vises til drøftelsen av det strafferettslige gjenstandsbegrepet i forhold til data i kapittel 4 i boken Lov og rett i Cyberspace, Fagbokforlaget 2005.

15 TOSLO-2004-84792. Dommen er rettskraftig.

For kopieringen av innholdet på produksjonsserveren og overføringen av anbudet, ble han domfelt for grov økonomisk utroskap, jf. strl. § 275, jf. § 276. Videre ble han domfelt for forsettlig overtredelse under særlig skjerpende omstendigheter av åvl. § 54, jf. § 43, for å ha kopiert databaser som var resultat av en større investering. Han ble også domfelt etter åvl. § 54, jf. § 2, for kopiering av noen datamaskinprogrammer og et skjermbilde. For dette utmålte retten en straff på fengsel i 6 måneder hvorav 120 dager betinget, og idømte erstatning til fornærmede med kr 85 900. Påtalemyndigheten fikk dermed gjennomslag for alle tiltaleposter unntatt en, som gjaldt overtredelse av tyveribestemmelsen for å ha borttatt data som tilhørte fornærmede. Rettens oppfatning var at data ikke kunne anses som gjenstand, og heller ikke kunne borttas, jf. strl. § 257. Denne sakstypen må forventes å bli vanligere fremover, siden store verdier i dagens bedrifter består av databaserte tjenester.

Hvis vi returnerer til problemstillinger som gjelder beskyttelsesbrudd, omgåelser og kodeknekking, må også strl. § 262 nevnes. Bestemmelsen kom inn på ledig plass i straffeloven i 1995,[16] og rettet seg opprinnelig mot ulovlig dekoding av betalingsbelagte tilgangskontrollerte kringkastingssignaler (radio og TV). Forarbeidene viste hovedsaklig til det særlige behovet for vern for slike tjenester, og til at åvl. § 54, jf. § 2, normalt ikke kunne anvendes selv om sendingene etter sin art var vernet etter åndsverkloven.[17] Det ble vist til at piratdekoding gjerne skjer til privat bruk, mens eneretten gjelder tilgjengeliggjøring overfor allmennheten, dvs. utenfor det private område.

Den såkalte Smartkort-dommen (Rt. 1995 s. 35) bekreftet at åndsverkloven ikke ga tilstrekkelig vern i slike tilfelle. Høyesterett opphevet herredsrettens domfellelse for krenkelse av eneretten, jf. åvl. § 54, jf. § 2. Domfelte hadde solgt 120 piratdekodingskort som dekodet betalingsbelagte TV-sendinger. Høyesterett drøftet først om salget av piratdekodingskort kunne anses som medvirkning til krenkelse av eneretten til tilgjengeliggjøring for allmennheten. Det ble lagt til grunn at bruk av piratdekodingskort gjerne skjer privat. Slik privat bruk kunne ikke innebære noen krenkelse av eneretten til å foreta tilgjengeliggjøring for allmennheten. Dermed kunne det heller ikke dømmes for medvirkning til krenkelse av eneretten. Et eventuelt medvirkningsansvar måtte ha bygget på at en kjøper skulle benytte dekodingskortet til å fremføre TV-sendingene utenfor det private området. Dette forelå det ikke holdepunkter for. Høyesterett drøftet videre om salget av de 120 kortene innebar en direkte overtredelse av eneretten til fremføring av TV-sendingene for allmenn-

16 Jf. lov av 17. april 1995 nr. 15.
17 Ot.prp. nr. 4 (1994-1995) s. 49 flg.

heten. Samlet sett representerte ikke kjøperne noen privat krets og sterke reelle hensyn talte for domfellelse. Høyesterett kom imidlertid til at det ikke forelå hjemmel for straff. Grunnen var at salg av kortene ikke kunne anses som fremføring. Det ble vist til at salgene i tid lå forut for TV-sendingene. Denne type piratdekoding ble først straffbar ved innføringen av strl. § 262 i 1995.

På bakgrunn av krav i tilgangskontrolldirektivet[18] og Europarådskonvensjonen om tilgangskontrollerte tjenester,[19] ble strl. § 262 vesentlig omarbeidet og området for det straffbare utvidet i 2001.[20] Etter endringen står bestemmelsen til vern om såkalte *"vernede tjenester"*, definert i bestemmelsens fjerde ledd. Tjenestene inndeles i tre grupper. Dette er betalingsbelagte tilgangskontrollerte radio- og TV-sendinger (bokstav a), informasjonssamfunnstjenester (bokstav b), og tilgangskontrollen i seg selv *"når den må regnes som en egen tjeneste"* (fjerde ledd i.f.). Hvis man ser bort fra den tredje kategorien, kan det vernede objekt kort beskrives som beskyttede data under overføring.

Strl. § 262 er en beskyttelsesbruddbestemmelse, jf. annet ledd, som rammer *"[d]en som ved bruk av dekodingsinnretning påfører den berettigede et tap eller skaffer seg selv eller andre en vinning ved å få uautorisert tilgang til en vernet tjeneste"*. Dette leddet uttrykker direkte hovedhensynet bak regelen, nemlig vernet om vederlagsinteressen. Ved uautorisert tilgang tapes betalingen for sendingen. Overtredelse av annet ledd, selve beskyttelsesbruddet, foretas gjerne av private brukere. Ved endringen i 2001 ble imidlertid tyngdepunktet i regelen forskjøvet til første ledd, som rammer befatning med dekodingsutstyr. Særlig har det vært et mål å slå ned på den profesjonelle profittmotiverte piratvirksomheten.[21] Denne dreining i fokus gjenspeiles i forskjell i strafferamme. Mens det rene beskyttelsesbrudd etter 1995-regelen ble straffet med bøter eller fengsel inntil 1 år, ble strafferammen for denne handlingen redusert til bøter eller fengsel inntil 6 måneder, ved endringen i 2001. Overtredelse av første ledd straffes imidlertid med bøter eller fengsel inntil 1 år. Etter første ledd bokstav a og b, rammes således forskjellige vinningsmotiverte handlinger som går ut på produksjon, spredning, utnyttelse og markedsføring av dekodingsinnretning. I tillegg rammes utbredelse eller forsøk på utbredelse av dekodingsinnretning, uten vinnings hensikt, jf. bokstav c. Også medvirkning er straffbart.

Både strl. 262 annet ledd og åvl. § 53a første ledd, rammer altså fremgangsmåter som populært har vært kalt "beskyttelsesbrudd". Ord som "be-

18 Direktiv 98/84/EF av 20. november 1998.

19 Europarådskonvensjon av 24. januar 2001 (178 ETS) on the Legal Protection of Services based on, or consisting of, Conditional Access. Norge undertegnet 24. januar 2004.

20 Jf. endringslov av 15. juni 2001 nr. 57.

21 Se Ot.prp. nr. 51 (2000-2001), bl.a. på s. 5 sp. 1 og s 15. sp. 1

skyttelsesbrudd" og "knekking" leder tanken hen på noe som brytes eller beskadiges. Imidlertid skjer logisk beskyttelsesbrudd som omgåelse eller misbruk av teknisk svakhet. Fremgangsmåten isolert sett innebærer ikke noen beskadigelse av objektet.

Åvl. §53a ligner på strl. § 262 ved at den både retter seg mot beskyttelsesbruddet (jf. *"å omgå"*, jf første ledd), og mot de tilretteleggende handlinger, dvs. befatningen med dekodingsutstyr og tjenester i den forbindelse (jf. listen i annet ledd). De to bestemmelsene er langt på vei overlappende i sin spesifikasjon av de tilretteleggende handlingene, se følgende sammenligning av alternativene i gjerningsbeskrivelsene:

Åvl § 53a annet ledd bokstav:

- a: "selge, leie ut eller på annen måte distribuere", smlg. "distribuerer, selger, leier ut" i § 262 første ledd bokstav a.

- b: "produsere eller innføre for distribusjon til allmennheten", smlg. "fremstiller, innfører" i § 262 første ledd bokstav a.

- c: "reklamere for salg eller utleie", smlg. "annonserer eller på annen måte reklamerer" i § 262 første ledd bokstav b.

- d: "besitte for ervervsmessige formål", smlg. "i vinnings hensikt…besitter" i § 262 første ledd bokstav a.

- e: "tilby tjenester i tilknytning til", smlg. "installerer, vedlikeholder eller skifter ut" i § 262 første ledd bokstav a.

Forskjellen i orddrakt skyldes nok langt på vei at de to bestemmelsene gjennomfører to forskjellige direktiver, og at man i begge tilfelle har valgt å prioritere nærhet til direktivteksten fremfor intern regelharmonisering. En uheldig konsekvens er at lovtekstene blir tungt tilgjengelige og det kan oppstå uklare grenseflater.

Videre kan det etter lovendringen som presiserer omfanget av eneretten i åvl. § 2 tredje, jf. fjerde ledd, reises spørsmål ved om det er noe behov for strl. § 262. Etter rettsoppfatningen i Smartkort-dommen ble slik dekoding sett på som privat bruk som var unntatt fra den opphavsrettslige eneretten. Dette rettslige utgangspunkt må imidlertid nå justeres for så vidt som dekodingen retter seg mot tjenester som er nevnt i åvl. § 2 fjerde ledd (se lovsitatet i kapittel 1). Bestemmelsen presiserer at denne form for fremføring omfattes av eneret-

ten. Det gjelder selv om fremføringen typisk skjer privat. Salg av piratdekodingsutstyr myntet på slike tjenester må følgelig være straffbart som medvirkning til overtredelse av eneretten. Rettsoppfatningen i Smartkort-dommen for så vidt gjelder medvirkningsansvaret kan derfor neppe lenger opprettholdes. Hvorvidt forholdet etter presiseringen i åvl. § 2 også kan rammes som en direkte krenkelse av eneretten, beror antakelig på fortolking av det såkalte nærhetskravet. Uansett gis det nå klar separat hjemmel for straff i spesialbestemmelsen i åvl. § 53a, annet ledd bokstav a, jf. § 54.

Nærhetskravet gjelder nærhet i sammenhengen mellom tjeneste/utstyr som inngår i leveringen av verket, og allmennhetens mulighet til å anskaffe verket nettopp via dette utstyret/tjenesten. Innholdet i nærhetskravet kan f. eks. drøftes i forholdet mellom dataterminalen på en internettkafé og nedlasting av verket, mellom et piratdekodingskort og adgangen til TV-sendingen , og mellom en musikktjeneste som iTunes og nedlasting av lydfilene.

3. Lovgivningsteknikken

Det vil ha fremgått at straffereglene for henholdsvis misbrukshandlingen og de tilretteleggende handlinger er fordelt på to forskjellige bestemmelser når det gjelder uberettiget adgang til data, se strl. § 145 annet ledd og § 145b. Dette er en annen lovteknikk enn den som er valgt for strl. § 262 og åvl. § 53a, hvor handlingstypene er bakt inn i forskjellige ledd i samme bestemmelse. Videre har lovgiver gitt et snevrere vern for data generelt enn for vernede tjenester/verk etter strl. § 262 og åvl. § 53a. Strl. § 145b ble som nevnt avgrenset til utelukkende til å gjelde spredning av *tilgangskoder* som kan gi tilgang til et datasystem. Befatning med *hackerverktøy* som også kan gi slik tilgang ble ikke kriminalisert. Begrensningen i området for strl. § 145b står i kontrast til den omfattende kriminaliseringen etter strl. § 262 første ledd og åvl. § 53a annet ledd, som både omfatter tilgangskoder og hackerverktøy, samt en rekke forskjellige befatningsformer i tillegg til spredning av dekodingsutstyret. Forskjellen i lovteknikk og området for det straffbare ble ikke kommentert under lovforberedelsen.

4. Mer om hensynene bak reglene

Med et fugleperspektiv på de nevnte bestemmelser kan det for det første konstateres at strl. § 145 annet ledd nå er en generell "datavernbestemmelse". Formålet med å fjerne beskyttelsesvilkåret var å bringe vernet om data mer på linje med vernet om fysiske gjenstander hvor det ikke oppstilles noe krav om beskyttelse (se f. eks. tyveri- og underslagsbestemmelsene, jf. strl. § 257 og

§ 255 første alt).[22] De eldre hensyn bak bestemmelsen må antas fremdeles å være gjeldende, så langt de passer. Etter forarbeidene er dette hensyn til vern om privatlivets fred, vern mot misbruk av data som er beskyttet og vern om det samfunnsmessige behov for et apparat som sikrer mulighet for utveksling av lukket informasjon.[23] I tillegg vernes vederlagsinteressen.[24]

Det kan imidlertid reises spørsmål ved om det er noe rom igjen for hensynet til vederlagsinteressen etter den siste lovendringen. Muligheten for å kunne oppnå vederlag for dataene er betinget av at de er beskyttet, slik at de ikke blir fritt tilgjengelige. Det kan synes kunstig å anvende strl. § 145 annet ledd på slike tjenester, når de ikke er uttrykkelig beskrevet i straffebudet. For de fleste betalingstjenester vil strl. § 262 være den relevante bestemmelse. Imidlertid foreligger det klare uttalelser i forarbeidene til strl. § 145 annet ledd om at betalingsbelagte data omfattes. Dette støttes også av uttalelser i den såkalte BetalTV-dommen (Rt. 1994 s. 1619). Disse momenter er belyst i neste kapittel. Strl. § 145 tredje ledd annet alternativ, gir dessuten hjemmel for straffskjerpelse for overtredelser av annet ledd som er begått i vinnings hensikt. Dette tilsier at annet ledd kan anvendes på krenkelser som rammer betalingsbelagte data. Likevel er det kanskje mer nærliggende å forstå bestemmelsen slik at straffskjerpelse vil være aktuelt når gjerningspersonen er ute etter data med en spesiell verdi, som f. eks. ved industrispionasje eller inntrengning i en database med kredittkortnumre som kan omsettes. Handlinger som utelukkende krenker vederlagsinteressen antas derfor å måtte bli vurdert etter andre regler enn strl. § 145 annet ledd. Bestemmelsen kommer imidlertid til anvendelse ved *irregulær tilgang* til datasystemer, også om de leverer vernede tjenester, jf. drøftelsen i neste kapittel. På grunn av teknologiutviklingen og datasikkerhetens økte betydning, er det i dag naturlig også å vise til de vanlige datasikkerhetskravene som selvstendige hensyn bak strl. § 145 annet ledd. Dette er hensyn til integritet, konfidensialitet, tilgjengelighet og autentisering. Også strl. § 145b skal bidra til å effektivisere dette vernet om data.

Strl. § 262 beskytter den avtalebaserte vederlagsinteressen og skal primært slå ned på profesjonelle vinningsmotiverte anslag mot denne. Åvl. § 53a skal effektivisere vernet om opphavsretten, og inneholder som nevnt en avgrensning i forhold til privat tilegnelse av verket på det som i alminnelighet oppfattes som *"relevant avspillingsutstyr"*. På det generelle plan har man i forarbeidene lagt til grunn at avtalevilkår vil være styrende for hva som er relevant avspil-

22 Se Innst.O. nr. 53 (2004-2005), Justiskomiteens merknader i pkt. 2.
23 Se NOU 1985: 31 Datakriminalitet s. 13.
24 Se Ot.prp. nr. 35 (1986-1987) s. 17.

lingsutstyr. Samtidig skal uttrykket forstås *"relativt fleksibelt"* og *"et sentralt moment i vurderingen vil være hvilke forventninger til avspilling forbruker med rimelighet kan ha til det aktuelle produkt"*. En annen sak er at lovgiver rent konkret har uttalt at en Mp3-spiller er relevant avspillingsutstyr for lydfiler solgt på CD.[25] Passusen *"det som i alminnelighet oppfattes som"* skaper uklarhet, fordi man neppe kan tale om én representativ oppfatning av hva som er relevant avspillingsutstyr. Tvert imot må det antas at oppfatningen varierer mellom miljøer, blant forskjellige rettighetshavere og forbrukere. I konkrete tilfelle vil trolig klare avtalevilkår ha betydning for avgrensningen. I online-forhold må slike avtalevilkår formidles elektronisk over nett, se også bestemmelsen i e-hl. § 11, om tjenesteyterens opplysningsplikt, som forutsetter dette.[26] For offline-produkter som CD og DVD, er påtrykte avtalevilkår på innpakningen det praktiske. Åvl. § 53a kan dermed innebære en renessanse for "shrink wrap"-klausulen som tidligere er blitt møtt med atskillig skepsis i norsk rett.[27]

5. Beskyttelsesbruddet og det vernede objekt

Strl. § 145 annet ledd verner om *"data og programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler"*.[28] Etter ordlyden omfattes både lagrede data (informasjon) og data under overføring (kommunikasjon). Det stilles ingen krav til dataenes innhold.

BetalTV-dommen (Rt.1994 s. 1610) avgjorde imidlertid at databegrepet måtte fortolkes innskrenkende i forhold til fjernsynssendinger/-program. Spørsmålet var om bestemmelsen kom til anvendelse på salg av piratdekodere beregnet på betalingsbelagte tilgangskontrollerte TV-sendinger, jf. medvirkningsregelen i strl. § 145 fjerde ledd. Høyesterett kom til at forholdet ikke ble rammet av bestemmelsen fordi fjernsynsprogram ikke var "data". Dette til tross for forarbeidenes uttalelse om at *"ordlyden er så vid at bestemmelsen også vil omfatte tilfelle hvor den datalagrede informasjon er tilgjengelig for*

25 Det vises til uttalelser i Ot.prp. nr. 46 (2004-2005) s. 119 sp. 1, og Innst.O. nr. 103 (2004-2005) s. 38-39.

26 E-handelsloven (e-hl.) er lov 35/2003.

27 "Shrink-wrap" betyr plastinnpakning. "Shrink-wrap"-klausuler er avtalevilkår som er trykt på eller lagt ved varen og som man ikke kan gjøre seg kjent med i sin helhet før innpakningen er brutt. Slike vilkår kan også komme opp som rulletekst ved avspilling av en DVD-film eller dataprogram. På nettet tales det om "web-wrap", "click"-wrap og "browse-wrap"-klausuler, dvs. vilkår som presenteres i forbindelse med at man anskaffer varen over nett. Vedtagelsesspørsmålet slike vilkår reiser må prøves mot e-hl. § 11.

28 Programutrustning er et underbegrep i forhold til det generelle "data". Se Ot.prp. nr. 35 (1986-1987) s. 20 sp. 1 og s. 26.

allmennheten mot erleggelse av betaling, og den innlagte sperre bare har til formål å sikre at betaling ytes... Også krenkelse av vederlagsinteressen vil derfor falle inn under strl. § 145 annet ledd".[29] Førstvoterende som representerte flertallet, viste til dette stedet i forarbeidene og mente at det ikke tok sikte på fjernsynsprogrammer, men på *"formidling av EDB-basert informasjon mot betaling, noe som ikke er uvanlig"*. Dommen ble avsagt under sterk dissens, men Høyesterett la uten videre flertallets fortolkning til grunn i den nevnte Smartkort-dommen (Rt. 1995 s. 35), som kom kort tid etter.

Den innskrenkende fortolkning er derfor klart fastslått for fjernsynssendinger/-programmer. Imidlertid viser uttalelsen til førstvoterende at strl. § 145 annet ledd ble ansett å verne om det som senere er blitt kalt "informasjonssamfunnstjenester". Således dekket man i 1995 ved innføringen av vernet om beskyttede kringkastingssignaler i strl. § 262, et tidligere helt straffritt område. Utvidelsen i 2001 til også å omfatte beskyttede informasjonssamfunnstjenester,[30] jf. fjerde ledd bokstav b, innebar på den annen side en direkte overlapping i forhold til det materielle virkeområdet for strl. § 145 annet ledd. Som yngre spesialregel går strl. § 262 foran strl. § 145 annet ledd, i slike tilfelle.

Helt enkelt er det likevel ikke. Visse harmoniseringsspørsmål reiser seg avhengig av *hvordan beskyttelsesbruddet begås*. Problemstillingen oppstår både i forhold til beskyttede kringkastingssignaler og informasjonssamfunnstjenester (online-tjenester), jf. § 262 fjerde ledd bokstav a og b. Begge definisjonene gjelder signaler under overføring, og beskyttelsesbruddet skal følgelig rettes mot denne kommunikasjonen. Tatt på ordet må den uautoriserte tilgangen etter annet ledd, arte seg som en form for rettsstridig tapping av signaler. I så fall må tapping skje når signalene likevel overføres til andre tjenestemottakere. Dette er praktisk i forhold til kringkastingssignaler som sendes ut på likt til et større antall mottakere, men passer ikke like godt for online-tjenester som overføres på individuell anmodning. I online-tilfellene er det antakelig mer praktisk at det skjer et datainnbrudd mot avsenderpunktet. Her vil dataene som skal overføres elektronisk, være lagret i påvente av en forespørsel fra tjenestemottakeren.

Siden dataene er lagret, oppstår spørsmålet om de omfattes av definisjonen i strl. § 262 fjerde ledd bokstav b. Definisjonen lyder: *"tjenester som telefor-*

29 Ot.prp. nr. 35 (1986-1987) s. 21.

30 Informasjonssamfunnstjenester er definert i e-hl. § 1 annet ledd. Det er definisjonsdelen i bokstav a som er relevant. Definisjonen inneholder ikke noe krav om bruk av tilgangskontroll eller koding. Dette er et tilleggsvilkår som er lagt til definisjonen av informasjonssamfunnstjenester i strl. § 262 fjerde ledd bokstav b. Definisjonen i e-hl. § 1 annet ledd, bygger på de to såkalte definisjonsdirektivene av 1998 nr. 34 og 48 EF. Nr. 48 inneholder også en liste ("Annex V") med en negativ avgrensning av begrepet.

midles elektronisk på forespørsel fra den enkelte tjenestemottaker, når tilgang i forståelig form er avhengig av tillatelse fra tjenesteyter og ytes mot betaling". Uttrykket *"teleformidles elektronisk"* tar sikte på datakommunikasjon, ikke på data som er lagret. Hvis lagrede data som skal danne grunnlag for en online-tjeneste ikke er beskyttet etter strl. § 262, oppstår spørsmålet om de kan anses å ha vern etter andre bestemmelser, nemlig strl. § 145 annet ledd eller åvl. § 53a. Anskaffelsen av dataene ville utvilsomt være uberettiget, jf. strl. § 145 annet ledd. Dersom fremgangsmåten hadde preg av å være en omgåelse av et effektivt teknisk beskyttelsessystem for et vernet verk, ville også åvl. § 53a kunne anvendes. Imidlertid antas det å være naturlig å legge størst vekt på ordet "tjenester" i definisjonen i strl. § 262 fjerde ledd bokstav b. Ordet kan forstås som noe mer enn data, dvs. som å omfatte hele det tekniske konsept som er nødvendig for å tilrettelegge data for sending på tjenestemottakerens bestilling. I så fall skal beskyttelsesbruddet henføres under § 262 annet ledd.

En annen problemstilling knytter seg til *metoden* for beskyttelsesbrudd. Grovt sett faller beskyttelsesbrudd i to kategorier. Den ene er *passordinnbrudd*, mens den andre er *irregulær tilgang*.[31] Det karakteristiske ved passordinnbrudd er at gjerningspersonen skaffer seg tilgang på ytelsen med en ulovlig erhvervet kode (tilgangskoder, passord, kodenøkler osv). Når beskyttelsen er satt til vern om et vederlagskrav, innebærer fremgangsmåten at tjenesteyteren går glipp av vederlaget. Beskyttelsesbruddet gir imidlertid ikke gjerningspersonen noen større adgang til ytelsen enn en autorisert bruker ville hatt, fordi passordtilgangen setter grenser for utnyttelsen av tjenesten. Det er nettopp denne situasjonen som er regulert i strl. § 262 annet ledd (se lovsitatet i kapittel 2). Forarbeidene forutsetter at passordinnbrudd vil være en vanlig fremgangsmåte som rammes av bestemmelsen. Det presiseres at legaldefinisjonen av dekodingsinnretning i strl. § 262 tredje ledd, også omfatter *"kodar, kodenøklar og passord",* samt *"PIN-kodar"*.[32]

Hvis beskyttelsesbruddet derimot skjer ved irregulær tilgang, er det karakteristiske at gjerningspersonen skaffer seg tilgang ved å utnytte en teknisk sårbarhet, *og trenger inn utenom begrensningene satt av tilgangskontrollen* (passordet). Irregulær tilgang oppnås ved bruk av hackerverktøy, som lovgiver ved behandlingen av strl. § 145b, valgte *ikke* å kriminalisere befatning med (se kapittel 1 og 3). Ikke sjelden oppnår hackeren kontroll på administratornivå, dvs. på et nivå som gjør at han har tilgang til alle ressurser som den aktuelle datamaskin har å tilby, f. eks. hele biblioteket av film, musikk og dataspill

31 Den som ønsker å lese mer om passordinnbrudd og irregulær tilgang, kan se i boken Lov og rett i Cyberspace, Fagbokforlaget 2005.

32 Se Ot.prp. nr. 51 (2000-2001) s. 14.

som ellers skulle lastes ned som enkeltfiler (eventuelt kringkastes) i henhold til en avtale støttet av teknisk tilgangskontroll. Irregulær tilgang gir således mulighet for utøvelse av dataskadeverk ved endring og sletting av innhold, utestengning av vanlige tjenestemottakere osv. Mens passordinnbruddet rammer vederlagsinteressen, er det karakteristiske ved irregulær tilgang at systemintegriteten rammes, dvs. at dataressursene som sådan taper beskyttelse mot uautoriserte handlinger.

Irregulær tilgang er en meget vanlig metode for å skaffe uberettiget adgang til data. Som eksempel kan det vises til to Høyesterettsavgjørelser i 2004, se Rt. 2004 s. 94 og s. 1619. I den førstnevnte saken skjedde inntrengningen på en web-server benyttet som vert for en elektronisk varslingstjeneste. Beskyttelsesbruddet skjedde ved kartlegging og misbruk av en teknisk sårbarhet, samt installering av en ny sårbarhet (”bakdør”) som senere ble misbrukt ved et par anledninger. Den uberettigede adgang ble blant annet benyttet til å slette data slik at varslingstjenesten ble satt ut av funksjon. I Rt. 2004 s. 1619 hadde to personer brutt seg inn på 437 servere i 33 land, ved bruk av hackerverktøy som utnyttet tekniske sårbarheter på serverne. På denne måten hadde de oppnådd ”root tilgang”, dvs administratorprivilegier. Tilsvarende metoder kan selvsagt også benyttes på servere som er verter for online-tjenester eller for data som skal kringkastes. Tjenesteyterens bekymring er i slike tilfelle antakelig primært konsentrert om integriteten og tilgjengeligheten av tjenesten, dvs. om den er i stand til å betjene vanlige kunder, om innholdet er intakt, om datasikkerhetstiltakene fortsatt er til å stole på osv. Tapet av vederlaget har mindre betydning. Dessuten innebærer ikke irregulær tilgang nødvendigvis noe tap av vederlag. Gjerningspersonens motiv kan ligge på en helt annen kant enn å skaffe seg gratis tilgang til materialet. Fra hackersaker er erfaringen at motivet kan gjelde ønske om status, om å skade, om å skaffe dataressurser for egne formål, skape uautoriserte nett, oppnå anonymitet osv. I slike tilfelle synes det mindre naturlig å anvende strl. § 262.

Derimot omfattes forholdet av strl.§ 145 annet ledd, supplert med strl. § 261 eller § 393. Strl. § 145 annet ledd står til vern om lagrede data generelt, herunder ”*programutrustning*”. Hackeres inntrengning på datasystemer med de motiv som er nevnt, innebærer en nyttiggjøring av dataressursene i videre forstand og rammer nettopp programutrustning og konfigurasjonskontroll. Det at beskyttelsesvilkåret ble fjernet endrer ikke noe på bestemmelsens anvendelighet på slike tilfelle.

Mens strl. § 262, med de forbehold som er gjort, primært verner data under overføring, verner strl. § 145 annet ledd og åvl. § 53a, både data som er lagret og data under overføring. For strl. § 145 annet ledd følger det uttrykkelig av ordlyden, mens åvl. § 53a gjelder omgåelse av tilgangskontroll på

vernede verk generelt, uavhengig av spredningsmetoden. For verk som overføres er det som tidligere påvist, stor grad av materielt sammenfall mellom strl. § 262 og åvl. § 53a. I forarbeidene til åvl. § 53a, vises det imidlertid til at strl. § 262 ikke er dekkende i forhold til forpliktelsene etter opphavsrettsdirektivet. Dette gjelder *"enkeltelementer i gjerningsbeskrivelsen"* og at straffelovens bestemmelser *"stiller krav om forsett"*.[33] Forarbeidene konkretiserer imidlertid ikke hvilke enkeltelementer som ikke dekkes av strl. § 262. På den annen side er overlappingen mellom gjerningsbeskrivelsene klar (se kapittel 2). Sanksjonskravet i opphavsrettsdirektivet art. 8, omfatter ikke et strafferettslig uaktsomhetsansvar, så heller ikke denne delen av begrunnelsen berettiger en særbestemmelse i åndsverkloven. Noen slik forpliktelse følger heller ikke av Cybercrime-konvensjonen art. 10 (opphavsrettskrenkelser). Bestemmelsen krever bare straffehjemmel for de forsettlige handlinger, jf. vilkåret *"wilfully"*. Dessuten krever verken direktivet eller konvensjonen at de folkerettslige forpliktelsene skal gjennomføres nettopp i åndsverkloven. Det kan derfor konstateres at de folkerettslige forpliktelser ikke er til hinder for en vesentlig samordning og forenkling av de norske bestemmelsene.

6. Kodeknekking

Tilgangskontroll baseres vanligvis på bruk av kryptering (koding). Tilgangskodene er derfor verdifulle for den som vil omgå beskyttelsen. Rettighetshaverne prøver å skjerme kodene på forskjellig vis, f. eks. ved jevnlig utskifting, eller ved skjermingstiltak som kryptering, implementering i hardware komponenter osv. Koder som blir kjent (kompromittert) blir ofte distribuert i piratmiljøer.

I en dom avsagt av Nedenes herredsrett 1. juli 1998,[34] ble en 40 år gammel mann domfelt for i løpet av ett og et halvt år å ha solgt ca. 29 000 smartkort til bruk for piratdekoding av betalTV-sendinger. Han solgte primært blanke kort og formidlet kodene slik at kundene selv kunne foreta kodingen og fortløpende oppdatere dem med nye koder når TV-selskapene skiftet dem ut. Han ble dømt for medvirkning til overtredelse av strl. § 262 (1995-bestemmelsen), til fengsel i 8 måneder og inndragning av vinning med kr. 1, 8 millioner.

En tilgangskode er en nøkkel som anvendes mot en lås (tilgangskontrollen). Tilgangskontrollen bygger på en algoritme som kan være kjent. Sikkerheten hviler på at nøkkelen holdes hemmelig. Nøklene må distribueres til brukerne slik at de kan skaffe seg lovlig tilgang, og i praksis gjøres det gjerne ved at

33 Ot.prp. nr. 46 (2004-2005) s. 113 pkt. 3.5.1.3.4.

34 Nedenes herredsretts sak nr. 98-00235 M. Dommen er rettskraftig.

nøkler er lagt inn i avspillingsutstyr, f. eks. i en TV-dekoder eller DVD-spiller. Nøkkelen kan også betros brukeren som avgir den til systemet, f. eks. brukernavn og passord som oppgis ved innlogging på et datasystem. I alle tilfelle er det tale om autentiseringsrutiner, hvor nøkkelen transporteres eller avgis til låsen, hvor den kontrolleres og godtas. Dette gir mange muligheter for å avdekke nøkkelen, både i utstyret hvor den er lagret, hos brukeren, og under transport til låsen, dvs. ved selve autentiseringen. En såkalt "sniffer" er et verktøy som kan tappe kommunikasjon, og anvendes gjerne for å registrere passord når de som del av autentiseringsrutinen kommuniseres til tilgangskontrollen (låsen). Bruk av "sniffer" uten tillatelse gir uberettiget adgang til data som overføres, og er straffbart etter strl. § 145 annet ledd. Det foreligger domfellelse for bruk av "sniffer" i den nevnte saken i Rt. 2004 s. 1619. Forholdet som gjaldt bruken av snifferen ble rettskraftig avgjort av tingretten.[35]

Tilgangskoder kan også avdekkes på annet vis enn ved tapping. Aktuelle metoder kan være "passordknekking", eventuelt analyse eller dekompilering av et program dersom nøkkelen er skjult i programmet. Passordknekking kan utføres maskinelt, f. eks. på basis av ordlister ("dictionary attack"), eller ved såkalt "uttømmende søk" ("brute force"). Dette er maskinell generering av tegnkombinasjoner i stort tempo for å finne kombinasjoner som er gyldige passord. Passordknekkingen forenkles hvis noen hemmelige parametre er kjent. Dersom man f. eks. har fått fatt i en gyldig kode, kan ofte resten av kodene til et system gjettes.

Problemstillingen som skal drøftes er om den aktiviteten som går ut på å skaffe seg passord er straffbar. Tilfellet med tapping av passord under kommunikasjon holdes utenfor som klart straffbart, jf. kommentarene ovenfor. Det antas dessuten at passordene er "data", jf. strl. § 145 annet ledd. Dette følger av begrepets generelle betydning, og er dessuten lagt til grunn av Borgarting lagmannsrett i den såkalte DVD-saken (RG. 2004 s. 414) (frifinnelse). Et av de spørsmål retten måtte ta stilling til, gjaldt at tiltalte hadde tatt del i passordknekking som hadde avdekket de beskyttede spillernøklene til det tekniske beskyttelsessystemet som var lagt på DVD-filmene. Beskyttelsessystemet het Content Scrambling System (CSS). En spillernøkkel hadde blitt avdekket ved dekompilering, fordi den hadde ligget ubeskyttet i et DVDspillerprogram for PC. Ved dekompilering ble kildekoden til spillerprogrammet og spillernøkkelen som lå i denne, kjent. Dette skjedde forut for tiltaltes befatning med saken. På grunnlag av denne spillernøkkelen ble det iverksatt passordknekking ved uttømmende søk, noe som ledet til at hele nøkkellageret til CSS ble kompromittert. Spørsmålet var om passordknekkingen kunne rammes av strl. § 145

35 Stavanger tingretts dom av 19. august 2003. Saknr 02-634 og 635 M.

annet ledd. Lagmannsretten mente at retten til nøklene måtte anses å være avledet av retten til filmen. Siden man hadde kommet til at tiltalte hadde rett til å begå beskyttelsesbrudd på sin egen DVD-film, mente retten at han også var berettiget til å knekke alle spillernøklene.

Lagmannsrettens begrunnelse rekker imidlertid ikke lenger enn til at det må være berettiget å skaffe seg tilgang til én nøkkel, den som er nødvendig for å skaffe fullstendig uhindret tilgang til sin egen film. Siden tiltalte allerede hadde en spillernøkkel, nemlig den som var avdekket ved dekompileringen av spilleren, hadde han ikke noe aktuelt behov for hele nøkkellageret. Her valgte imidlertid retten å ta hensyn til at tiltalte kunne komme til å få behov for flere nøkler i fremtiden.

Relevansen av mulige fremtidige behov synes å være noe tvilsom. Videre kan et slikt avledet vern som retten baserte sitt resonnement på, innebære et incitament til selvtekt, noe rettsordenen vanligvis ikke anerkjenner. Det oppstår også andre uheldige virkninger, ved at en kode som er blitt kjent kan benyttes ikke bare på eget, men også på andres beskyttede innhold. Koden kan f. eks. anvendes til å dekryptere og tilegne seg ikke bare filmer man eier, men også filmer man leier. Dersom et beskyttelsessystem er basert på et endelig antall nøkler, kan det dessuten anses å være beskadiget dersom alle nøklene blir knekket. Høyesterett har ikke hatt foranledning til å uttale seg om spørsmålet og rettstilstanden kan vel antas å være noe usikker.

I henhold til de nye reglene i avl. § 53a er det imidlertid etablert visse grunnlag for kodeknekking. Utgangspunktet er at kodenøkler som inngår i effektive tekniske beskyttelsessystemer, jf. første ledd, er *"innretninger"* eller *"komponenter"* som kan rammes av forbudene i åvl. § 53a annet ledd. Forbudene i annet ledd vil typisk slå til dersom kodene tilgjengeliggjøres direkte, eller legges inn i programvare som benyttes til å omgås effektive tekniske beskyttelsessystemer. Kodeknekking som aktivitet, rammes således av produksjonsalternativet i åvl. § 53 annet ledd bokstav b. Etter denne bestemmelsen gjelder imidlertid forbudet bare når produksjonen skjer *"for distribusjon til allmennheten"*. Kodeknekking som skjer for å støtte private omgåelseshandlinger er derfor ikke forbudt. Forutsetningen er at produksjonen ikke skjer med en plan om å spre kodene til almennheten. Selve spredningshandlingen rammes uansett av åvl. § 53a annet ledd bokstav a, mens kodeknekking med en plan om å spre til almennheten, rammes av bokstav b. Det gjelder enten spredningen skal skje direkte, f. eks. ved at kodelister distribueres på pratekanaler på internett, eller indirekte, f. eks. ved at kodene legges inn i omgåelsesprogramvare som i sin tur distribueres til almennheten. Verken produksjons- eller spredningshandlingen blir lovlig fordi den som (planlegger å) spre(r) opererer med en forutsetning om at de som laster ned bare skal nyttiggjøre verktøyene til privat bruk.

Denne reguleringen begrunnes i forarbeidene. I lovproposisjonen står det blant annet at *"forslaget bør avgrenses mot de rent private handlinger. Ettersom besittelse av omgåelsesverktøy ikke vil være forbudt med mindre den har ervervsmessige formål, vil heller ikke forbudet mot produksjon og import av slike innretninger gjelde for de rent private handlinger"*.[36] Departementets syn fikk tilslutning av flertallet i komitéen i Stortinget, og den endelige utformingen av åvl. § 53a annet ledd, ble vedtatt i samsvar med departementets forslag.

I tillegg inneholder åvl. § 53a et generelt unntak fra forbudene i bestemmelsen, for *"forskning i kryptologi"*. Dette er i samsvar med punkt 48 i fortalen til opphavsrettsdirektivet, og er reelt begrunnet i at slik aktivitet innebærer analyser som også kan avdekke hemmelige koder. Ifølge lovproposisjonen kan det reises spørsmål om når en aktivitet er slik at den kan kalles *"forskning"* slik begrepet er benyttet i åvl. § 53a. Tilknytning til en forskningsinstitusjon er ikke et vilkår. På den annen side er det heller ikke slik at *all* aktivitet knyttet til kryptologi innen en forskningsinstitusjon, nødvendigvis er å anse som forskning. Det bemerkes at det er *"under enhver omstendighet innholdet i arbeidet som skal vurderes, ikke rammene rundt det"*.[37] Hvis det først er på det rene at det foreligger forskning i bestemmelsens forstand vil det også være adgang til å foreta kodeknekking, i den utstrekning dette er relevant innen forskningsarbeidet.

Rettspolitisk har det hersket usikkerhet om hvor ønskelig det er å straffbelegge kodeknekking mer generelt. Frykten gjelder at strenge regler skal virke hemmende på teknologiutviklingen, fordi forskning på algoritmer og kryptering anses å være vesentlig for utviklingen. Dette er grunnen til det eksplisitte unntaket for forskning i kryptologi i åvl. § 53a tredje ledd, som nevnt. Også i forarbeidene til endringen av strl. § 262, i 2001, ble spørsmålet berørt. Justisdepartementet var skeptisk til et forbud mot å knekke en kode. Det ble uttalt at *"konsekvensene av et slikt forbud er imidlertid svært usikre, og kan komme i strid med f eks åndsverkloven §§ 39h og 39i, samt prinsippene om retten til "omvendt utvikling" ("reverse engineering"). Sistnevnte rettighet antas å ha vært viktig i utviklingen av stadig ny datateknologi*".[38]

På den annen side har ikke dette hensynet vært forstått å gå så langt at enhver kan tilegne seg konkrete programopplysninger slik han selv vil. Det er tale om å finne en balanse mellom kryssende hensyn. På bakgrunn av program-

36 Spørsmålet om lovligheten av befatning med omgåelsesverktøy er drøftet på sidene 118-121 i Ot.prp. nr. 46 (2004-2005). Sitatet er hentet fra s. 121 sp. 1. Se også Innst.O. nr. 103 (2004-2005) s. 39.

37 Ot.prp. nr.46 (2004-2005) s. 121 pkt. 3.5.1.5.5.

38 Ot.prp. nr. 51 (2000-2001) s. 12.

varedirektivet[39] er det inntatt regler i åvl. § 39h og § 39i, som regulerer adgangen til å analysere og dekompilere et program. Ifølge åvl. § 39h tredje ledd, er den som har rett til å bruke et datamaskinprogram berettiget til å *"iaktta, undersøke eller prøve ut hvordan programmet virker"*. Retten gjelder bare for *"å fastslå idéene og prinsippene som ligger til grunn for de enkelte deler av programmet"*. Dette er i tråd med den vanlige avgrensningen for opphavsretten, som gjelder verkets konkrete utforming, ikke de idéer og prinsipper som verket er bygd på. Dette presiseres i fortalen til programvaredirektivet, hvor det står at *"for at det ikke skal oppstå tvil må det presiseres at det bare er et datamaskinprograms uttrykksform som er beskyttet, og at de idéer og prinsipper som ligger til grunn for de enkelte delene av programmet, herunder de som ligger til grunn for programmets grensesnitt, ikke er opphavsrettslig beskyttet etter dette direktiv. I samsvar med dette prinsippet om opphavsrett og i den utstrekning logikk, algoritmer og programmeringsspråk utgjør idéer og prinsipper, er ikke disse idéene og prinsippene beskyttet etter dette direktiv."*

Derimot er konkret informasjon som utgjør programmets uttrykksform, beskyttet. Tilsvarende er adgangen til å foreta dekompilering nøye regulert i åvl. § 39i, etter de samme prinsipper. l forhold til tilgangskoder legger reglene således opp til at man lovlig kan analysere hvordan algoritmen som skaper "låsen" fungerer, men at man ikke kan gå så langt som til å liste ut nøklene til låsen. Nøklene er ikke idéer og prinsipper, men konkrete komponenter i verket som må anses opphavsrettslig vernet.

Kultur- og Kirkedepartementet har også noen overveielser om dette i Ot.prp. nr. 46 (2004-2005), s. 122-123. Spørsmålet gjelder om spillerprogram kan anses som datamaskinprogram som kan være lovlig gjenstand for omvendt utvikling, jf. åvl. § 39h og § 39i. Hvis de ikke er datamaskinprogram, kan retten til omvendt utvikling, herunder dekompilering, fritt begrenses ved avtale. Dermed økes vernet om dekodingsnøklene når de er lagt inn i programmet. Departementet viser til at spørsmålet må avgjøres *"etter en konkret vurdering i det enkelte tilfellet"*.

Programvaredirektivets prinsipper synes å være forenlig med et vern om tilgangskodene. Et straffebud som uttrykkelig tar konsekvensen av dette, er strl. § 262, som bestemmer at tilgangskontrollen anses som en vernet tjeneste når den må regnes som egen tjeneste, se fjerde ledd i.f. Et beskyttelsesbrudd mot tilgangskontrollen vil jo jevnlig gå ut på å avdekke koder. Tilgangskontrollen har derfor allerede et eksplisitt strafferettslig vern når den er satt på tjenester som nevnt i strl. § 262.

39 Direktiv 91/250/EØF.

CSS er et slikt selvstendig system. Strl. § 262 var likevel ikke aktuell i DVD-saken, fordi saken gjaldt beskyttelsesbrudd på offline produkter (DVD-filmer) som faller utenfor definisjonen av vernet tjeneste, jf. strl. § 262 fjerde ledd.

I lys av strl. § 262 er det ikke unaturlig å tolke strl. § 145 annet ledd slik at tilgangskodene har et selvstendig vern mot uberettiget adgang. Ordlyden dekker i hvert fall forholdet. Etter den siste endringen av bestemmelsen er det likegyldig om adgangen skaffes ved beskyttelsesbrudd eller ei. Spørsmålet er kun om man er berettiget til tilgangskoden. Her synes lagmannsretten som nevnt å ha gått noe langt i DVD-dommen i å anse tilgang berettiget. På den annen side taler sammenhengen med strl. § 145b *mot* at strl. § 145 annet ledd fortolkes slik at kodeknekking omfattes. Strl. § 145b rammer kun den som *sprer* tilgangsdata som kan gi adgang til et datasystem. Siden Stortinget valgte ikke å kriminalisere *anskaffelse* eller *fremstilling* av tilgangsdata (se kapittel 1), lot man passordknekking være straffri i forhold til denne bestemmelsen. Hensynene til sammenheng mellom bestemmelsene og til en lojal oppfølgning av lovgivers intensjoner uttrykt ved behandlingen av strl. § 145b, tilsier at strl. § 145 annet ledd må fortolkes innskrenkende på dette punkt, slik at kodeknekking heller ikke omfattes av denne bestemmelsen. Motargumentet er at det fremstår som en lakune at kodeknekking som avdekker passord til datasystemer skal være straffritt, mens tilsvarende handling for så vidt gjelder vernede tjenester og verk, rammes etter fremstillings- og produksjonsalternativene i strl. § 262 første ledd bokstav a og åvl. § 53a annet ledd bokstav b. Det er ikke mindre grunn til å sikre datasystemer generelt enn datasystemer som leverer vernede tjenester eller verk.

En annen begrensning i strl. § 145b, er at den bare rammer spredning av tilgangskoder til et *"datasystem"*. Dette er et annet uttrykk enn *"data og programutrustning"* som er benyttet i strl. § 145 annet ledd. Strl. § 145b omfatter klart koder som er nødvendige for å få tilgang til arbeidsstasjoner og servere i et nett. Et annet spørsmål er om koder som er nødvendig for å få tilgang på krypterte data lagret på en periferienhet (harddisk, CD-R. DVD, USB-penn) omfattes. Kodene gir tilgang til *"data"* og misbruk av slike koder rammes av strl. § 145 annet ledd. Sammenhengen mellom bestemmelsene tilsier at slike koder også anses å være omfattet av strl. § 145b, til tross for ordet *"datasystem"*. Dessuten bygger begrepet *"datasystem"* på Cybercrime-konvensjonens definisjon i art. l (a), som omfatter både prosessoren og periferienhetene. Art. 6 som er grunnlaget for strl. § 145b, pålegger kriminalisering av tilgangskoder som gir tilgang til *"hele eller deler av"* et datasystem. Alternativet *"deler av"* er falt ut ved den norske implementeringen, kanskje fordi det har vært tatt for gitt at man ikke nødvendigvis får tilgang på et helt system ved en enkelt inntrengning. Dataenes plassering (lokasjon) kan imidlertid sies å være på en del

av datasystemet, og tilgang oppnås ved dekryptering. Slik forstått dekkes også koder som dekrypterer innhold, av spredningsforbudet i § 145b.

7. Heleri av tilgangskoder

Tilgangskoder har en verdi i piratmiljøer, og kan også omsettes. Dette aktualiserer bruk av heleribestemmelsen i strl. § 317, som rammer befatning med utbytte av en straffbar handling. Det kan vises til to saker til illustrasjon. I den såkalte PINkode-kjennelsen (Rt. 1995 s. 1872) ble det domfellelse for kjøp av PIN-koder som kunne benyttes til å misbruke telefonanlegg for oppringninger uten betaling. Domfelte hadde antatt at kodene i utgangspunktet var anskaffet ved straffbare handlinger. Dette lot seg ikke konkret bringe på det rene, men hans subjektive oppfatning ble lagt til grunn og han ble domfelt for forsøk på heleri, jf. strl. § 317, jf. § 49. Om kodene uttalte Høyesterett at de *"gir tilgang til telefonselskapenes tjenester, og de har derved økonomisk betydning og er egnet til å bli disponert over. En PINkode må derfor anses som et utbytte i straffeloven § 317 første ledds forstand"*.

Som et eksempel fra underrettspraksis kan det vises til Nedre Romerike tingretts dom av 25. november 2003.[40] Domfelte, en 25 år gammel mann, var i besittelse av 650 000 brukernavn og passord som stammet fra en norsk bedrift. Retten vurderte forskjellige mulige primærforbrytelser og uttalte at den *"finner det utenkelig at noen legalt har tatt med seg 650 000 brukernavn og passord ut av bedriften av tjenestelige grunner eller at det har skjedd i vanvare"*. Resultatet ble domfellelse for overtredelse av strl. § 317.

Mottak av tilgangskoder fra en annen vil regelmessig kunne rammes på grunn av de straffesanksjonerte spredningsforbudene (primærforbrytelsene) i strl. § 145b, § 262 første ledd bokstav a og c, og åvl. § 53a annet ledd bokstav a.

8. Politiets rolle og det rettspolitiske fokus

Man kan spørre hvilken rolle politiet skal ha i forhold til pirateri og hacking. Under gjeldende kriminalpolitiske og budsjettmessige rammebetingelser, er effektiv bekjempelse via straff utelukket. Med forbehold for Datakrimavdelingen i Nye Kripos mangler politiet kompetanse og ressurser til å forfølge saker. Statistikken viser da også at bare et fåtall saker av denne art forfølges strafferettslig, kanskje med unntak av overtredelse av strl. § 262, hvor det pr. april 2005 er registrert 1010 forhold siden 1997. Ca. 800 av forholdene gjelder imidlertid én politiaksjon i Hordaland i 1997, hvor mange personer ble bøte-

40 Sak nr. 03-007516MED-NERO. Dommen er rettskraftig.

lagt for TV-pirateri. Etter utvidelsen av bestemmelsen i 2001 er bare 21 forhold registrert. En positiv fortolkning av statistikken er at lovlydigheten har bedret seg, men det finnes åpenbart andre mindre gunstige tolkingsmuligheter også.

Det er ikke dermed sagt at politiet ikke foretar seg noe. Ni av de 21 senere sakene har endt med helt eller delvis ubetinget straff, de fleste av de øvrige med bot. I forhold til internettrelatert pirateri avsa dessuten Oslo tingrett fellende dom den 12. november 2004, mot to menn som på gjerningstidspunktet var 24 og 25 år gamle *("Drink or Die-dommen")*.[41] Drink or Die var et internasjonalt piratnett med opprinnelse i Moskva. Deltagere i flere land har blitt domfelt, blant annet i England og USA. Deltagerne knekket beskyttelsen på programvare, dataspill, film og musikk, testet pirateksemplarene og gjorde piratvaren (warez) tilgjengelig på internett. Begge de tiltalte ble domfelt for overtredelse av spredningsforbudet i åndsverkloven. Den ene hadde fungert som "sikkerhetssjef" i piratmiljøet, dvs. vedlikeholdt "botnettet" som opprettholdt pratekanalen som ble benyttet i samarbeidet mellom deltagerne i piratgruppen. Dommen lød for begge på fengsel i 120 dager, samt bot kr 3000. Den ene ble i tillegg idømt et erstatningsansvar til rettighetshaverne med kr 20 000.

Det kan også vises til Oslo tingretts dom av 27. mai 2005.[42] En 36 år gammel mann, ble idømt samfunnsstraff i 120 timer, subsidiært fengsel i 120 dager for medvirkning til overtredelse av åndsverkloven, ved å etablere og drifte en "hub" for spredning av piratvare, på fildelingstjenesten Direct Connect.

For øvrig savnes et klart politisk og lovgivningsmessig fokus både for hvilke handlinger som anses straffverdige og i forhold til hva som faktisk er gjort straffbart. Området for det straffbare er nemlig svært vidt. De folkerettslige forpliktelsene til å ramme pirateri gjelder overtredelser som skjer *"on a commercial scale"*, jf. TRIPS-avtalen art. 61 og Cybercrime-konvensjonen art. 10. Uttrykket er oversatt med henholdsvis *"i kommersiell målestokk"* (TRIPS) og *"i et kommersielt omfang"* (Cybercrime-konvensjonen). Straffebudene går imidlertid langt utover den folkerettslige forpliktelsen til å kriminalisere overtredelser, ved at de rammer *enhver* overtredelse, stor eller liten, og etter åvl. § 54, til og med små overtredelser i sin uaktsomme form.[43] Dette til tross for at det etter Cybercrime-konvensjonen er tilstrekkelig med straff bare for de forsettlige overtredelser, jf. art. 10. Dertil har det siden 1990-tallet pågått en global utvikling av nettverksteknologien som leder til at en stadig større del av

41 TOSLO-2003-19164.

42 TOSLO-2004-94328

43 Se også strl. § 391a (naskeri) hvoretter også helt små krenkelser av den type som ellers faller inn under strl. § 262, omfattes.

krenkelsene begås av enkeltindivider med tilgang på en datamaskin. Bruken av fildelingstjenester er helt sentralt for piratanskaffelser. Selv om man kan konstatere at enkelte tjenester har svært mange deltagere, kjennetegnes aktiviteten av at deltagerne er anonyme, ikke kjenner hverandre og at det hele foregår på et privat individuelt nivå uten annet fortjenestemotiv enn å spare utgiftene til et lovlig kjøp av verket.[44] Mens kriteriet *"on a commercial scale"* nok passer godt på industrielt pirateri som foregår i stor utstrekning i andre deler av verden, må den nettbaserte kriminaliteten utført av enkeltindivider anses som et hovedproblem her hjemme. I forhold til slik kriminalitet er ikke betegnelsen *"on a commercial scale"* opplagt treffende, samtidig som det store antallet lovbrytere representerer en formidabel kapasitetsmessig utfordring for politiet. Intet for tiden tilsier at dette vil bli gitt håndhevelsesmessig prioritet.

Hvis man holder fast på at problemet skal løses ved rettslige virkemidler, gjenstår spørsmålet om man ikke burde gi rettighetshaverne - de fornærmede - større muligheter til å forfølge krenkelsene etter eget valg, f. eks. som en erstatningssak, når de likevel ikke kan få hjelp av politiet. Rettighetshaverne må i så fall få adgang til utlevering av sporingsdata fra internettilbyderne på linje med politiet, ellers vet de ikke overfor hvem de kan rette et søksmål. Etter e-komloven[45] § 2-9- tredje, jf. fjerde ledd, kan slike data bare gis til politiet, påtalemyndigheten eller retten. Men i tredje ledd siste punkt, åpnes det for utlevering av sporingsdata også til andre, forutsatt at det gis en bestemmelse om det. Dette kunne f. eks. vært gjort ved en tilføyelse i åndsverkloven. En slik løsning kunne anses som god forebyggende kriminalpolitikk, ved at man slipper å strafforfølge unge lovovertredere, samtidig som man gjennom erstatningsansvaret oppnår en oppdragende effekt. Siden jeg allerede kan høre protestene på vegne av personvernet, iler jeg til med en presisering: Tilgang til sporingsdata kan sammenlignes med tilgang til data i telefonkatalogen, bare at man er henvist til en opplysningstjeneste hos tilbyder i stedet for et åpent oppslagsverk. Etterforsking i form av avhør, ransaking og beslag, skal forbli en politioppgave. Poenget er at tilgang på sporingsdataene gjør det mulig for fornærmede å ivareta sine rettigheter uten å innlede straffesak.

44 I artikkelen Hvem laster ned musikk, Dagbladet 6. april 2005, ble det vist til en undersøkelse hvor det fremgår at tre av ti norske ungdommer laster ned tilnærmet all musikk de skaffer seg (gratis), og halvparten laster ned 70% av musikken. Kun få musikkanskaffelser blant ungdom gjøres mot betaling.

45 Lov 83/2003.

12 JURISDIKSJON OG AVGRENSNING AV INTERNETT`S KOLLIDERENDE HANDLINGSUNIVERSER

Georg Philip Krog[1]

Formålet med artikkelen er å skissere et strategisk teknisk og juridisk handlingsprogram for hvordan grenseoverskridende interaksjoner over Internett kan reguleres av ett forutbestemt sett av konsistente rettsnormer. Artikkelen vil ved hjelp av et konstruert eksempel illustrere den aktuelle problemstillingen.

Hvordan kan et institutt ved Universitetet i Oslo, f.eks. Nordisk institutt for sjørett (heretter A), tilby fra Norge (heretter T1) en læringsmodul i internasjonal maritim rett ved interaktive bestillingstransmisjoner over Internett til spesielt utvalgte land (heretter T2) og samtidig avgrense mot andre utland (heretter T3)?

Eventuelt, hvordan kan A tilby og avgrense modulen fra T1 til hhv profesjonelle advokater (heretter B) og mot forbrukere, f.eks. studenter (heretter C) i T2?

Vi forutsetter at læringsmodulen innehar tekniske og/eller innholdsmessige feil således at B påføres skade og lider tap, eller at B tilbyr samme modul til andre som ikke har kontrahert med A således at A lider tap.

Innledningsvis beskriver artikkelen Internett som et territorialt uavgrenset nettverk, og angir konsekvensfølgene av at A tilbyr læringsmoduler over Internett.

For det første kan digitale interaksjoner medføre multijurisdiksjonelle tilknytninger og virkninger.

For det andre kan et rettsforhold være medlem av like mange rettssystemer som der er suverene stater således at rettssystemene konkurrerer om å regulere, dømme og utøve makt over rettsforholdet.

For det tredje kan rettssystemene angi motstridende handlingsuniverser.

Uten territoriell avgrensning av internasjonal interaksjon og rettslig avgrensning av rettsforhold, kan overholdelse av rettsnormer i en stat represen-

---

1 Universitetsstipendiat, Institutt for rettsinformatikk, det juridiske fakultet, Universitetet i Oslo. Artikkelen er en utvidet versjon av artikkelen "Internett, jurisdiksjon og territoriell avgrensning" publisert i Lov&Data, Nr. 1/2005, s. 24-27.

tere brudd på rettsnormer i en annen stat. Rettsbrudd kan sanksjoneres, og eventuelt anerkjennes og fullbyrdes i utlandet. (Kap. I)

Artikkelen søker videre å gi svar på hvordan A som avsender av et tilbud fra T1 kan anvende sin autonome kompetanse til å konstruere tekniske metoder som positivt tillater og dermed aksepterer interaksjon med B som interagerer fra T2, eller negativt forbyr og dermed avviser interaksjon med C som interagerer fra T3.

Ambisjonen er å lokalisere interaksjonen til definerte stedskoordinater og/ eller relativisert til utvalgte individer.

Som det fremgår kan avgrensningen foregå positivt, negativt eller i en kombinasjon.

Avgrensningen kan bestå i å gi/ ikke gi seg selv tilgang til eller motta/ikke motta henvendelse fra definerte stedskoordinater på bestemte eller ubestemte tider.

Valgene av avgrensningsmåte(r) og steds- og tidskoordinat(er) kan få betydning for ulike aspekter av spørsmålene om internasjonal domstolskompetanse (og rettsvalg) (kap II).

Artikkelen gir videre forslag til hvordan A kan anvende sin autonome kompetanse til å vedta vernetingsavtaler.

Formålet med vernetingsavtaler er å avgrense suverene staters potensielt konkurrerende rettssystemer, og eksklusivt tilordne en bestemt domstol kompetanse til å realitetsavgjøre en sivil og kommersiell tvist som har oppstått eller måtte oppstå i et bestemt kontraktsrettsforhold.

Ambisjonen er å lokalisere rettsforholdet til et forutbestemt normsystem med en gitt rettslig normmengde hvor motstridende handlingsuniverser for hva som er forbudt, påbudt eller fritatt er eller metodisk kan elimineres (kap III).

I fortsettelsen angir artikkelen konsekvensen av at tekniske og juridiske avgrensningsmetoder er kjent ugyldig eller ikke er anvendt. I så fall blir rettsgrunnlaget for juridisk avgrensning konvensjonelle regler om domstolskompetanse (kap IV).

Artikkelen angir så hvordan A kan anvende sin autonome kompetanse til å vedta rettsvalgsavtaler.

Formålet med rettsvalgsavtaler er å avgrense og utpeke anvendelig materiell rett som rettsgrunnlag for den kompetente domstol til å realitetsavgjøre en potensiell tvist.

Ambisjonen er kort å påpeke rettsvalgsbegrensningene (kap V).

Endelig beskriver artikkelen hvordan enkelte avgrensningsmetoder kan konstrueres slik at sivile og kommersielle tvister delvis transformeres fra å kvalifiseres som medlem av den internasjonale privattrett til også å henføres under internasjonal offentlig rett, herunder strafferett, som bedømmes etter domstollandets interne rett.

Slik kan avsenderen forutberegne at domstollandets strafferett får anvendelse, og på visse betingelser kan transformasjonen gi større grad av forutberegnelighet over hvor det sivile krav kan pådømmes (kap VI).

Artikkelen avrundes med noen hypoteser om det internasjonale søksmålsklima (kap. VII).

I Globalt nettverk, globale virkninger, konkurrerende rettssystemer og kolliderende handlingsuniverser

1 Rettsbevissthet om jurisdiksjonsrisikoen

Internett`s globale nettverk har aksentuert risikoen for å bli saksøkt av mottakere i andre land enn landet hvorfra A trådløst eller trådbundet overfører digitale tegn. Problemet har gitt incitament til å kartlegge virksomheters rettsbevissthet om jurisdiksjonsrisikoen. Den hittil mest omfattende undersøkelsen[2] ble gjennomført i tidsrommet fra august til november 2003 av tre initiativtakere[3] og publisert i april 2004. Artikkelen innleder med den empiriske undersøkelsen og hvilke problemer som ble identifisert. I korte trekk viste undersøkelsen følgende:

- Blant de juridiske problemer relatert til e-handel mente majoriteten av virksomhetene at den mest alvorlige og bekymringsfulle risikofaktor var risikoen for å bli saksøkt i utlandet med grunnlag i internasjonale regler om domstolsjurisdiksjon i sivile og kommersielle saker.
- Selskaper i Nord-Amerika var mer bevisste og bekymret for jurisdiksjonsrisikoen enn selskaper i Europa og Asia.
- Media-sektoren, uansett geografisk plassering, samt selskaper i Nord-Amerika hadde i størst grad tilpasset virksomheten i respons til jurisdiksjonsrisikoen.

2 Undersøkelsen ble gjennomført av i 45 land blant 277 små, medium og multinasjonale selskaper på tvers av alle selskapssektorer. Undersøkelsen kan i sin helhet lastes ned fra WIPO's nyhetssider: http://www.wipo.int/enforcement/en/news/2004/enforcement_10_12.html

3 The American Bar Association's Business Law Section, Cyberspace law Committee, International Chamber of Commerce og Internet Law and Policy Forum.

- Tilpasningene for å minimere risikoen for å bli saksøkt i utlandet eller i landet hvor virksomhetene var etablert og hadde sete besto hovedsakelig i å anvende såvel tekniske som rettslige virkemidler.
- De vanligste *tekniske virkemidlene* for å avgrense tilknytning til et bestemt territorium var å avgrense hvortil informasjon *fra* virksomhetene *til* brukeren geografisk skulle overføres. De vanligste avgrensningsmetodene var å tilgjengeliggjøre 1) nasjonal relevant informasjon 2) på nasjonalt språk, 3) på nasjonal server, 4) under nasjonalt toppdomene, 5) samt å kreve brukerens selvregistrering av hvor brukeren er bosatt eller er statsborger og/eller 6) å benytte teknisk software registrering om hvorfra brukeren interagerer. Som følger kan avgrensningsmetoden enten være positivt å tillate og dermed akseptere, eller negativt å forby og dermed avvise overføring.
- De vanligste *juridiske virkemidlene* for å avgrense og tilordne et rettsforhold til et forutbestemt forum var å anvende vernetingsavtaler (enten ved click-wrap agreement eller generelt utformet terms of use).

2 Globalt nettverk og konsekvensfølger

Bakgrunnen for avgrensningsbehovet er Internett`s territorialt uavgrensete informasjons- og kommunikasjonsnettverk.

I det globale nettverket tilbys ulike typer av IK-tjenester. Tjenestene tillater representasjon av ulike ytringshandlinger,[4] ulike grader av interaktivitet[5] og et mangfold av funksjoner.[6]

Den "tradisjonelle" [7] transmisjons- og retransmisjonsprosessen i nettverket består i ytringshandlinger[8] som på et eller flere lagrings- eller representa-

4 Lyd, tekst, still eller levende bilde, multimediekarakter.

5 For eksempel resiprok utveksling av informasjon mellom avsender og mottaker (transmisjon og retransmisjon) eller ensidig transmisjon fra avsender til mottaker.

6 Eksempelvis kommunikasjon, underholdning, informasjon, transaksjon.

7 Nye og antatt fremtidsdominerende handelsformer kan endre dette bildet, feks elektroniske agenter som kommuniserer seg selv gjennom nettet ved å reprodusere og overføre en eller flere kopier av seg selv for å forhandle med andre agenter, databaser etc. Se Bing, Jon, Electronic agents and intellectual property law, Artificial Intelligence and Law, 2004, s. 39-52, spesielt s. 44.

8 Ytringshandlingenes fiksering til og representasjon i digitale koder utgjør en binær datamengde som kan ha kvalitativ informasjonsverdi.

sjonsmedier fikseres til og representeres i digitale tegn.[9] De digitale tegnene kan kopieres,[10] og kan trådbundet eller trådløst overføres[11] til et eller flere andre lagrings- eller representasjonsmedier.

Prosessen kan foregå mellom én avsender og én mottaker, mellom den opprinnelige mottakeren som nå fungerer som avsender til en annen mottaker, eller mellom flere avsendere og mottakere. Videre er prosessen repeterbar. Endelig kan prosessen ofte gjennomføres til selvvalgt sted og tid.

Som følger kan transmisjons- og retransmisjonsprosessen foregå fra punkt til punkt, fra punkt til multipunkt, mutlipunkt til punkt, eller multipunkt til multipunkt[12] og over territorielle landegrenser.

Således kan A´s ytringshandling som fysisk er utført på T1 medføre direkte, indirekte, kvantitative, kvalitative, faktiske eller potensielle *virkninger* både nasjonalt, regionalt og globalt, og etablere en *kontakt* eller *tilknytning* til T2 og T3.[13]

Transmisjons- og retransmisjonsprosessen kan etablere rettsforhold over landegrenser som har deontisk status i relasjon til hvert enkelt av T2`s og T3`s rettssystemer.

På den ene siden er handlingen fri i relasjon til rettssystemer hvor rettsforholdet ikke er medlem. På den annen side er handlingen, når den er medlem av et rettssystem, enten påbudt, forbudt eller fri etter de fire pliktmodalitetene påbud, forbud, tillatelse og fritagelse.

---

9 I den lange utviklingslinjen av regionalt utviklete grafiske språk - en utvikling fra figurative bilder til såkalte piktogrammer, ideogrammer, og fonogrammer hvor symboler representerte selve lyden - er dataspråk(ene) et nytt og raskt oppfunnet globalt språk som kan representere både akustiske og grafiske språk. Det grafiske språks utvikling fra bilde til fonogram, og fra komplisert til forenklet grafisk formede symboler, har hatt nær sammenheng med skriveredskapene, mediet skriften har blitt fiksert til og etterhvert kravet til skriftspråkets effektivitets- og hurtighetskrav.

10 Digital privat reproduksjon har eller formodes å få større utbredelse enn analog privat reproduksjon, og har eller vil få store økonomiske konsekvenser, spesielt når der eksisterer store variasjoner mellom forskjellige lands vederlagsordninger for rettighetshavernes tap. Fra rettighetshavernes perspektiv taler dette for å gi en bred definisjon av de handlinger som er omfattet av reproduksjonsretten.

11 Se Europa-Parlamentets og Rådets direktiv 2001/29/EF av 22. mai 2001 om harmonisering av visse aspekter av opphavsrett og beslektede rettigheder i informationssamfunnet, fortalens pkt. 23.

12 Betydningen for artikkelens eksempel er kraftig forøkelse av den grenseoverskridende utnyttelse av intellektuell eiendomsrett. Utnyttelsesgraden kan skisseres mellom fem infohabitanters (repeterbare) transmisjoner og retransmisjoner. Dersom hver enkelt overfører og mottar én gang til/fra de fire andre, foreligger i alt 20 overføringer.

13 Forskjellen mellom nasjonal og internasjonal tilknytning kan være et enkelt tastetrykk, nemlig tasten som iverksetter kommandoen "overfør".

De fire pliktmodalitetene har fire tilsvarende former for rettslige pliktnormer som henholdsvis angir om en handling positivt er påbudt, negativt er forbudt eller tillatt (dvs ikke forbudt) eller fritatt (dvs ikke påbudt).[14]

Som følger kan et rettsforhold potensielt være medlem av like mange rettssystemer[15] som der er suverene stater.

Videre følger at rettssystemene kan konkurrere om å regulere, dømme og utøve makt over et rettsforhold som reises mellom de samme parter, har samme gjenstand[16] og hviler på samme grunnlag[17] (se figur 1).[18]

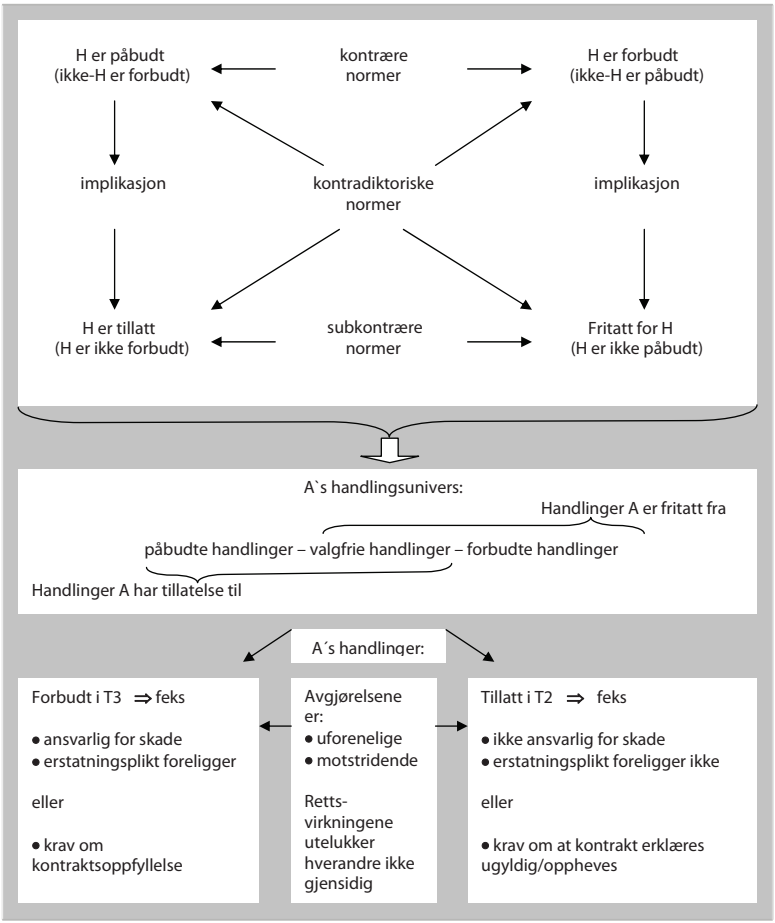
14 Pliktnormene kan reduseres og angi et tredelt handlingsunivers fordelt på om en handling positivt er påbudt, negativt er forbudt eller er valgfri. De fleste rettssystemer er basert på en uskreven metanorm som foreskriver at alt som ikke er forbudt ved særskilt norm er tillatt, og alt som ikke er særskilt påbudt er man fritatt fra.

15 Normgrunnlaget for territorielt å avgrense staters myndighet til å gi lover, avsi dommer eller utøve makt er tredelt. For det første kan normgrunnlaget være selvpålagt av suverene stater. For det andre kan normgrunnlaget være frivillig vedtatt av suverene stater ved harmoniserende konvensjoner og modellover. For det tredje kan normgrunnlaget være pålagt en suveren stat fra en overnasjonal lovgivende autoritet. På tvers av de tre normgrunnlag kan vi skille mellom rettsnormer som er positivt regulert ved lov eller rettsnormer som har grunnlag i ulike typer av praksis.

16 Med "gjenstand" sikter jeg til hva kravet gjelder.

17 Med "grunnlag" sikter jeg til de faktiske omstendigheter og den rettsregel som påberopes til støtte for kravet.

18 Såkalt positive kompetansekonflikter.



Figur 1. Karakteristisk for artikkelens eksempel er situasjonen der en part har anlagt sak ved en domstol med påstand om erleggelse av en ytelse i hht en internasjonal on-line kjøpekontrakt, mens medkontrahenten senere anlegger sak mot selgeren i en annen stat med påstand om at samme kontrakt erklæres ugyldig eller oppheves. Herav følger indirekte at partene er de samme uavhengig av partenes stilling i hver av de to saker, således at saksøkeren i den først anlagte sak kan være saksøkt under den senere anlagte sak.

En annen karakteristisk situasjon er at en part har anlagt sak ved en domstol med påstand om ansvar for påstått skade og at han plikter å betale erstatning, mens motparten senere anlegger sak i en annen stat med påstand om at fastsettelse av at han ikke er ansvarlig for skaden som fourutsetningsvis er en påstand om at erstatningsplikten bestrides.

Fra rettssystemenes perspektiv kan vi observere tre forhold: For det første kan rettstvister mellom de samme parter, med samme gjenstand og grunnlag parallelt versere for domstolene i forskjellige land da reglene om internasjonal domstolskompetanse kan være uensartede i nasjonale lovgivninger.

For det andre kan samarbeidet mellom stater variere i å koordinere deres respektive domstolers judisielle funksjon for unngå usammenhengende og innbyrdes motstridende avgjørelser i situasjoner med selvstendige saksanlegg i forskjellige land mellom de samme parter med samme gjenstand og grunnlag. Således vil rettsavgjørelsene kunne fullbyrdes særskilt.

For det tredje kan domstolene treffe uforenelige og motstridende avgjørelser. Følgen kan være at rettsavgjørelser ikke anerkjennes i utlandet fordi rettsavgjørelsen er uforenelig med en avgjørelse mellom de samme parter med samme gjenstand og grunnlag truffet i den stat anerkjennelsesbegjæring rettes til.

Fra A`s perspektiv observerer vi at mangelen på uniformerte regler om internasjonal domstolskompetanse kan lede til at A`s handlinger bli regulert av flere normmengder.

Ulike normmendger kan etablere motstridende handlingsuniverser hvor motstrid verken er eliminert eller metodisk kan elimineres. Som følger vil A oppleve koordinasjonsproblemer: hvilket normsystem skal A følge og bryte?[19]

Spørsmålet blir hvordan A så vidt som mulig kan, og straks fra begynnelsen av å rette et tilbud til andre land over Internett, vil kunne forhindre kolliderende og konkurrerende rettssystemer og motstridende handlingsuniverser.

Hvordan kan A avgrense og tilordne et rettsforhold til ett rettssystem (eller flere rettssystemer) med en gitt eller ideell[20] mengde normer som etablerer et forutberegnelig univers av påbudte, valgfrie og forbudte handlinger hvor motstrid er eliminert eller metodisk[21] kan elimineres?

Den ovenfor angitte årsak, følge og problem aksentuerer betydningen av tekniske og juridiske avgrensningsmetoder for adekvat å redusere mulige verdener, oppnå rettslig forutberegnelighet ved normkonsistens, og tillate eller forby bruk av overførte digitale tegn etter hva som er kompatibelt med et utvalgt rettssystems rettsnormer.

---

19 Koordinasjonsproblemet er spesielt akutt ift den autonome kompetanseutøvelse til å binde seg selv ved dispositive utsagn fordi personlige kontraktsløfter og -forpliktelser gir individet anledning til å fastsette, endre eller oppheve sin egen normative status. Se Herrestad, Henning, Formal Theories of Rights, 1996, pkt 3.3.

20 Se Herrestad, Henning, Formal Theories of Rights, 1996, hvor Herrestad i pkt 2.5.1 introduserer Stig Kanger`s deontiske logikk. Forutsetningen for at deontisk logikk skal fungere (for rettssystemer) er at normmengden er gitt. Med andre ord kan ikke flere normmengder konkurrere om anvendelse.

21 Kollisjon mellom rettsregler kan løses etter såkalte prioritetsregler med preg av retningslinjer (lex posterior, lex specialis og lex superior).

II Tekniske avgrensningsmetoder

1 Teknisk avgrensning

A som intereagerer fra T1 kan benytte deontisk automatiserte beslutningsprosesser etter flere avgrensningsmetoder.

Enten kan A programmere seg selv til positivt å tillate og dermed akseptere og inkludere interaksjon med B som interagerer fra T2. Således kan den deontisk automatiserte beslutningsprosessen gi tillatelser til A og B. For det første kan A gis tillatelse til både tilgang til T2 og B, og adgang til å motta henvendelse fra T2 og B. For det andre kan B gis tillatelse til tilgang til A.

Eller A kan progammere seg selv til negativt å forby og dermed avvise interaksjon med C som interagerer fra T3. Således kan den deontisk automatiserte beslutningsprosessen gi forbud til A og B. For det første kan A gis forbud både mot tilgang til T3 og C, og adgang til å motta henvendelse fra T3 og C. For det andre kan C gis forbud mot tilgang til A.

Den positive avgrensningen egner til å åpne, isolere og lokalisere interaksjon, kontakt, tilknytning og potensiell kontrahering til definerte territorier (stedskoordinater) og/eller et u/definert utvalg av potensielle medkontrahenter[22] til en u/definert tid (tidskoordinat).[23]

Den negative avgrensningen egner til å lukke, blokkere, forhindre, avslå, ekskludere og avvise interaksjon med de ikke positivt definerte territorier eller potensielle medkontrahenter. Således kan A unngå potensiell (global) kontakt og tilknytning som potensielt kan kvalifisere like mange rettssystemer anvendelige som der eksisterer stater.

De deontisk automatiserte avgrensningsmetodene om å akspetere T2 og B og avvise T3 og C kan anses som en todelt beskyttelsesrett.

A har primært rett til å ekskludere alle, eller bestemte territorier, og/eller alle eller bestemte personer.

A har sekundært rett til å forhindre de ekskluderte fra å handle bortsett fra personer som er unntatt fra eksklusjon.

Eksklusjonsretten kan være beskyttet etter to metoder.

---

22 Feks kontrakt sluttet av person for formål som må anses å ligge innenfor eller utenfor hans yrke eller erversmessige virksomhet (hhv forbruker, ikke-forbruker).

23 Avgrensningsmetoder kan sees under andre synsvinkler enn domstolskompetanse. Den norske stats lovgivende kompetanse kan bestemme hva som kvalitativt eller kvantitativt er forbudt eller valgfritt å overføre av informasjon til og fra norsk territorium. Videre kan den norske stats utøvende kompetanse iverksette og fullbyrde tiltak som faktisk begrenser informasjonsoverføringer til og fra norsk territorium.

Primært kan eksklusjonsretten være beskyttet med krav kun mot de som ved kontrakt er unntatt fra eksklusjon.

Sekundært kan eksklusjonsretten være beskyttet med krav om ikke-aksess mot alle som ikke er unntatt fra eksklusjon.[24]

Således kan A kontrollere eller styre de relevante tilknytningskriteriene som kan kvalifisere et rettssystem anvendelig. Med andre ord kan A teknisk avgrense, forutbestemme eller kontrollere og påvirke territorielle og/eller gruppebestemte makro- og mikrouniverser med en gitt mengde normer ihht A`s autonome kvalifikasjon av hvilke rettssystemer A teknisk utvelger positivt, negativt eller i kombinasjon.

a Tekniske geo-lokaliseringsverktøyer

Flere selskaper tilbyr ulike tekniske løsninger for å identifisere fra hvilket territorium brukeren interagerer, men hittil foreligger ingen standardisert og sikker teknisk løsning.

Verktøyene tillater å identifisere lokalisering skjult og ensidig[25], eller i åpenhet og med brukerens samtykke.

Mange rettssystemer forbyr innsamling, registrering, sammenstilling, lagring osv[26] av informasjon om en bruker med mindre et grunnlag fritar fra forbudet.

Forbudsnormen kan av styringshensyn være omfattende slik at lovgiver kan presisere de frie handlinger ved spesifikt å angi hva som er fritatt. Fritak er i mange rettssystemer basert på brukerens samtykke eller ved lov.

På den ene siden er disse pliktnormene relativt enkle å forholde seg til når en virksomhet anvender teknologi som kun behandler identifikasjonsdata lokalisert i virksomhetens hjemland. På den annen side kan like mange pliktnormer foreligge som der er suverene rettssystemer når identifikasjonsdata er lokalisert i utlandet og krever overføring til virksomhetens hjemland for å fastslå brukerens geografiske lokalisering. Hvilket lands pliktnormer som her

24 Formelt kan vi omtale rett til digitale tegn og områder som en rett til eklusjon, mens materielt kan vi omtale hvilke interesser digital eiendom tjener som kan være en rett til bruk.

25 Global Unique Identifier (GUID) som nå er fjernet fra feks Microsofts software produkter hvor et unikt nummer for produktet ble overfort under online registreringsprosessen sammen med brukernavn, addresse osv. Microsoft kunne identifisere brukere ved å sjekke brukerens GUID med informasjonen lagret i Microsofts Database. Intel anvendte en liknende løsning for å identifisere brukere online ved deres Processor Serial Number (PSN).

26 Se her personopplysningsloven § 2,2.

får anvendelse avgjøres av rettsvalgsregler,[27] som feks i Norge bestemmes av personopplysningsloven nr. 31/2000 § 4, annet ledd.[28]

Dersom tekniske lokaliseringsverktøyer kombineres med digitale sperrer (se pkt. d) som blokkerer ut uønskede brukere fra bestemte territorier, kan virksomheten positivt velge hvilke territorier de tillater kontakt med eller negativt avgrenser kontakt mot.

Et nytt normsett kan få anvendelse dersom en avvist bruker bryter den digitale sperren. Den rettslige følgen av brudd på digitale sperrer er ulikt utformet i forskjellige rettssystemer, feks sanksjonert med straff, ugyldighet etc (se kap. VI).

b Selvidentifisering[29]

Når A har identifisert territoriet brukeren interagerer fra, har A behov for å klassifisere i hvilken egenskap eller kapasitet brukeren interagerer for enten positivt å tillate og dermed akseptere, eller negativt forby og dermed avvise kontraktsinngåelse med bestemte medkontrahenter.

Behovet for avgrensning skyldes blant annet at flere lands rettssystemer beskytter forbrukere og umyndige med internasjonalt tvingende jurisdiksjons- og rettsvalgsregler.

27 Også kalt lovvalgsregler.

28 InfoSoc direktivets fortale pkt 57 fastslår at elektroniske opplysninger om forvaltning av opphavsrett samlet i tilknytning til rettighetsforvaltning kan, avhengig av deres utforming, samtidig behandle personopplysninger om individuelle forbruksmønstre mht beskyttede frembringelser og muliggjøre kortlagring av onlineadferd. Beskyttelse av personopplysninger etter Europa Parlamentets og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger bør inngå i tekniske beskyttelsesforanstaltningers funksjoner.

29 Selvidentifisering kan enten gjennomføres off-line (eksempelvis ved å innsamle opplysninger om kredittkort i kombinasjon med bostedsaddresse og telefonnummer) eller on-line selvidentifisering, enten med eller uten uavhengig og teknologisk verifisering om informasjonen som er avgitt er korrekt. Om verifisering av identiteter, se Risnes, Rolf "Electronic agents and PKI in the "Lovely Rita" scenario", publisert i THE LAW OF ELECTRONIC AGENTS, Complex 4/03, s. 51-66.

Jeg nevner spesielt forbrukerrettstvister. Som hovedregel[30] pådømmes slike tvister i forbrukerens bostedsland[31] og avgjøres etter dette domstollandets materielle rett.[32] [33]

For å unngå søksmål i forbrukerenes bostedsland, kan A anvende en prosedyre for selvidentifisering. I selvidentifiseringsprosedyren plikter brukeren å informere i hvilken egenskap han eventuelt vil kontrahere (forbruker eller ikke, myndig/umyndig etc), hvor han er domisilert og eventulet hvorfra han interagerer.

---

30 Reglene kan i noen rettssystemer fravikes ved avtale, se feks Brussel- og Luganokonvensjonen Artikkel 15 og Brusselforordningen Artikkel 17. 15. og 18. april 2005 vedtok EU Kommisjonen to proposisjoner (COM(2005) 145 final og COM(2005) 146 final) for beslutning i Rådet om å autorisere signering og ratifikasjon av to avtaler mellom EU og Danmark. Danmark deltar for tiden ikke i Title IV av Traktaten. Derfor er Danmark ikke bundet av de vedtatte instrumenter innenfor det juridiske samarbeidet i sivile saker, feks Brussel I forordningen. Således gjelder Brusselkonvensjonen mellom Danmark og EU, mens Brussel I forordningen gjelder mellom alle EU-landene bortsett fra Danmark. Danmark har ved flere anledninger uttrykt at de ønsker å delta i Brussel I forordningen. Kommisjonen tillot eksepsjonelt å utvide anvendelsen av Brussel I forordningen til også å omfatte Danmark. Begrunnelsen var det sterke ønsket om å etablere/opprettholde uniform lovgivning i EU. Liknende avtale ble inngått mellom Danmark og EU vedrørende forordning 1348/2000 on the service in the Member states of judicial and extrajudicial documents . Avtalene gir nærmere bestemte klausuler om 1) EF-domstolens rolle som autoritativ tolker, 2) mekanismer som muliggjør at Danmark kan akseptere Rådets fremtidige endringer av instrumentene og implementering av tiltak iverksatt under Traktatens Artikkel 202, 3) at avtalene termineres dersom Danmark nekter å akseptere slike fremtidige endringer og implementeringer, 4) Danmark`s forpliktelser i forhandlinger med tredjeland i saker som faller inn under avtalenes virkeområder, 5) si opp avtalene ved nærmere bestemt notifikasjon.

31 Se bl.a. Brussel og Luganokonvensjonen Artiklene 13 og 14, Brusselforordningen Artikkel 15. Om Brusselkonvensjonen Art. 13 nr. 3, se Foss, Morten and Bygrave, Lee, International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law, International Journal of Law and Information Technology, 2000, 8/2; Stone, Peter, Internet Consumer Contracts and European Private International Law, Information and Communication Technology Law, 2000, 9. Om Luganokonvensjonen Art 13 nr. 3, se see Foss, Morten, Rettslig Klassifisering av Digitale Produkter og Nettsteder – eksemplifisert ved Luganokonvensjonens Bestemmelser om Forbrukerkjøp, Complex 9/03. Om Brusselforordningen Art. 15.3, annet alternativ, se Krog, Georg Philip, The Brussels I Regulation Article 15.1c) - Whereto are commercial or professional activities directed through the Internet?, Yulex 2004, s. 117-148; Øren, S. T., Joakim, International Jurisdiction over Consumer Contracts in e-Europe, International and Comparative Law Quarterly, 2003, Volume 52, p. 676 and International Jurisdiction and Consumer Contracts – Section 4 of the Brussels Jurisdiction Regulation, Complex 5/04.

32 Se bl.a. Romkonvensjonen av 19. juni 1980, Artikkel 5.

33 Med andre ord kan ikke partene avtale at potensielle rettstvister kan eller skal pådømmes i andre land eller avgjøres etter andre lands materielle rettsregler enn hva de preseptoriske reglene bestemmer.

A avviser og forbyr kontraktsinngåelse basert på forbrukerens bosted og kostnadene (og sannsynligheter) for søksmål i utlandet.

Følgelig bør kontraheringsprosessen integrere et globalt uniformt selvregistreringsskjema som dekker forbrukerbegrepet på kryss av ulike rettssystemer.

Selvidentifisering kan enten gjennomføres prekontraktuelt eller kontraktuelt hvor selvidentifiseringen implementers som en inkorporert del av kontrakten.

På den ene siden har ingen plikt til å registrere opplysninger og kontrahere. Denne tredje pliktmodaliteten - at hverken påbud eller forbud foreligger - er aktuell når medkontrahenten unnlater å utføre selvregistrering av opplysninger. Unnlatelse av selvregistrering kan føre til automatisert avvisning fra kontrahering.

På den annen side kan kontrakten påby medkontrahenten positivt å måtte registrere korrekte opplysninger. Snudd kan man si at det er forbudt for medkontrahenten å registrere mangelfulle eller falske opplysninger i selvidentifiseringsprosedyren. Med andre ord foreligger ingen frihetsnormer for medkontrahenten til å registrere mangelfulle eller falske opplysninger i selvidentifiseringsprosedyren. Et manglende påbud impliserer at unnlatelsen av å registrere opplysninger er tillatt. Tilsvarende impliserer manglende forbud at man er fritatt fra å registrere opplysninger.[34]

Dersom teknisk selvidentifisering kombineres med digitale sperrer (se pkt. d) som avviser brukere med bestemte egenskaper, kan virksomheten positivt velge hvilke brukere de tillater kontakt med eller negativt avgrenser kontakt mot.

Et nytt normsett kan få anvendelse dersom medkontrahenten registrerer falske opplysninger. Den rettslige følgen av å registrere falske opplysninger er ulikt utformet i forskjellige rettssystemer, feks sanksjonert med straff, ugyldighet etc (se kap. VI).

c Territorielle markører

Virksomheter som signaliserer sine kommersielle handelsaktiviteter over Internett, informerer om varen/tjenesten og betingelsene for transaksjon ensidig og uten forhandling. Således styrer informasjonen i stor grad det psykologiske spillet mellom virksomhetens tilbud og en medkontrahents aksept.

Informasjonen kan være rettet til bestemte land eller persongrupper enten synlig eller skjult.

---

34 Det er meningsforskjeller om man språklig, ved bruk av en pliktnorm, skal formulere selvidentifiseringsprosedyren som et påbud eller forbud, eventuelt begge deler. Påbudsformen er gjerne anvendt når en medkontrahent ønsker å etablere en plikt for den andre medkontrahenten til å utføre en aktiv handling (her registreringen), mens forbudsformen gjerne anvendes når en medkontrahent ønsker å etablere en plikt for den andre til å unnlate noe.

Markørene for landsbestemt eller gruppebestemt informasjon kan - ved siden av tekniske geo-lokaliseringsverktøyer (ofte skjult), selvidentifiseringsfasen, digitale sperrer (ofte skjult), vernetingsklausuler,[35] leveringsstedsklausuler, rettsvalgsklausuler, den aktuelle informasjons- og kommunikasjonsservice,[36] - være informasjonens innhold, karakter og språk, samt betalingsmiddel, forsendelsestilbud etc (se kap. IV).

d Digitale sperrer

Både geo-lokalisering og selvregistrering kan som nevnt være kombinert med en digital sperre. Den digitale sperren kan avvise og forhindre den potensielle medkontrahenten i å fortsette kontraheringsprosessen frem til bindende kontrakt.

På den ene siden forbyr ikke de fleste rettssystemer ved en særskilt norm anvendelsen av digitale sperrer. Følgelig er anvendelsen av digitale sperrer som regel tillatt. Mange rettssystemer påbyr heller ikke ved en særskilt norm å anvende (bestemte) digitale sperrer. Følgelig kan man fritt velge mellom hvilke digitale sperrer man ønsker å anvende.

På den annen side forbyr mange rettssystemer brudd på digitale sperrer og angir ulike sanksjoner, feks sanksjoner som straff (se kap. VI).

2 A`s autonome kompetanse til teknisk avgrensning

A kan fastlegge de potensielle medkontrahentene B`s og C`s handlingsmønstre på to måter.

Enten har A kompetanse til å befale B og C til ikke å oppgi uriktig informasjon i selvidentifiseringsprosedyren (kap. II pkt. a), og ikke bryte den digitale sperren som skal forhindre tilgang til feks et webområde hvor tilbudet er tilgjengeliggjort (kap. II pkt. d).

Eller A kan ha autonom kompetanse til å binde seg selv, og avgi et tilbud som de potensielle medkontrahentene B og C ihht sin autonome kompetanse kan akseptere.

De to måtene å fastlegge et handlingsmønster er innbyrdes uavhengige, og kan derfor ikke kumuleres og reduseres til hverandre.

De fleste rettssystemer gir ikke avsenderen A av tilbudet autonom kompetanse til å befale, men snarere autonom kompetanse til å binde seg selv til å akseptere B og avvise C.

35 Er en ugyldig vernetingsklausul relevant?

36 Feks webadresser som ender på .no til forskjell fra .com.

Således kan A`s autonome kompetanse til å rette et tilbud mot territorium T2 anses som en tillatelse, samtidig som A`s autonome kompetanse til å avgrense tilbudet mot territorium T3, anses som et forbud.

3 Følgen av A`s tekniske kompetanseutøvelse

Interaksjonsaksepten eller -avvisningen for hhv B og C vil respektivt gi B og frata C mulighet til å anvende sin autonome kompetanse til å akseptere A`s avgitte tilbud.

B og C verken gis eller fratas en rett da B`s og C`s relasjon til A er avhengig av A`s autonome kompetanse og kompetanseutøvelse.

Når A aksepterer interaksjon med B, utøver A sin autonome kompetanse ved å avgi et tilbud som direkte binder A, samtidig som B avgir en aksept som direkte binder B.

Den autonome kompetanseutøvelsen pliktnormerer A og B til å oppfylle avtalens fastsatte handlingsmønster dersom avtalen er rettslig bindende.

Når A avviser interaksjon med C, binder A seg selv til ikke å motta C´s aksept. A befaler således ikke at C skal unnlate å avgi aksept, men A fratar C muligheten til å benytte sin autonome kompetanse.

A`s fratagelse av C´s mulighet til å benytte sin autonome kompetanse til å binde seg selv ved å avgi aksept kan kombineres med imperativer og pliktregler. Enten kan A forby C å aksessere A`s webside og kontraheringsområde. Eller A kan påby C å forlate A`s webside og kontraheringsområde.

4 Positiv og negativ teknisk avgrensning

Om A velger positiv avgrensning og aksept av B som primærfunksjon, vil den positive avgrensningen simultant implisere negativ avgrensning og avvisning av C som en følge og sekundærfunksjon, og vise versa.

Begge alternativer kan velges som primærfunksjon, og da vil ingen logisk sekundærfunksjon følge (fordi sekundærfunksjonen konsumeres av den kontrære primærfunksjonen).[37]

Valget av de tre alternativene kan få konsekvenser for hvilken domstol som tilordnes domstolskompetanse (se kap. IV).

37 Se Herrestad, Henning, Formal Theories of Rights, 1996, pkt. 3.5 om "Strong and weak deontic notions".

5 Avgrensningsmåter for teknisk å motta/ikke motta og sende/ikke sende

Interaksjonsaksept og -avvisning kan foregå på flere måter.

Enten kan A programmere seg selv til å bli gitt tilgang til T2. Eller A kan programmere seg selv til å motta henvendelse fra T2.

Videre kan enten A programmere seg selv til ikke å bli gitt tilgang til T3. Eller A kan programmere seg selv til ikke å motta henvendelse fra T3.

Endelig kan A kombinere de angitte beslutningsprosessene for interaksjonsaksept og -avvisning.

6 Stedskoordinatet for teknisk avgrensning

Interaksjonsavvisningen kan programmeres til å foregå på ulike statsterritorier.

Betydningen av hvilken avgrensningsmetode som er anvendt for å utføre interaksjonsaksept og -avvisning, samt stedet avgrensningsmetoden er anvendt er minst èn.

Avgrensningsmetodene er i noen stater patenterbare forretningsmetoder.[38] Tvister om erstatning for internasjonale krenkelser av patenterte avgrensningsmetoder tilordnes i flere rettssystemer til domstolen i staten hvor skaden ble voldt eller inntrådte, eller til domstolen i staten hvor patentet er registrert.[39]

Således feiler paradoksalt nok formålet med avgrensningsmetodene som nettopp er å unngå å bli saksøkt i utlandet (selv om grunnlaget for søksmålet nå er forskjellig).

7 Tidskoordinatet for teknisk avgrensning

Som det fremgår av kap. II pkt. 2 er tidskoordinatet for når avtaleprosedyren mellom A og B gir B en rett ift A resultat av at A´s kompetanse og kompetanseutøvelse gir opphav til en rett for B først etter

1. tilbudet er formulert i en språkhandling,
2. en rettslig norm kvalifiserer tilbudet som et rettslig dispositivt tilbud,
3. tilbyderen påtar seg en forpliktelse gjennom tilbudet,
4. en rettslig norm kvalifiserer påtakelsen av forpliktelsen som rettslig bindende,
5. tilbudet er eksponert til en mottaker,

38 Patentet kan gis en bred og eksklusiv rett for oppfinneren slik som er vanlig i USA.

39 Se Bing, Jon, Electronic agents and intellectual property law, Artificial Intelligence and Law, 2004, s. 39-52, som påpeker de interlegale problemene ift elektroniske agenters anvendelse til å utføre elektronisk handel, se spesielt s. 42 (patenter), s. 44 (opphavsrettigheter) og s. 46 (databaser).

6. mottakeren aksepterer tilbudet,
7. en rettslig norm kvalifiserer aksepten som en rettslig dispositiv aksept.
8. Først etter disse overgangene kan man tale om at det aksepterte tilbudet er blitt en pliktgrunn og en forpliktelse blir aktuell.[40]

Flere stater tilordner sine domstoler domstolskompetanse til å realitetsavgjøre saker som er *relatert til* kontrakt basert på at en forpliktelse har oppstått uten formell avtaleinngåelse. I såfall kan flere rettssystemer i spørsmålet om internasjonal domstolskompetanse utelate og anvise punktene 1 til 7 til realitetsavgjørelsen.

Det følger at A bør avvise C før A`s tilbud blir eksponert til C (feks ved bruk av geo-lokaliseringsverktøyer, selvidentifisering og digitale sperrer, se hhv kap. II pkt. a, b og d).

III Juridisk avgrensning av rettssystemer

1 Juridisk avgrensning

De fleste rettssystemer angir[41] normer om hvilke domstoler som i sivile og kommersielle saker er i rettslig posisjon til ved normeringsakter å fastsette, endre eller oppheve generelle eller individuelle normer ved å avsi dommer.[42]

40 Avtalen vil i såfall også representere en kompetansetildeling ved at medkontrahenten B gis kompetanse til å disponere over det overdratte kontraktsobjektet på en valgfri eller forbudt/påbudt måte.

41 Domstolskompetansen kan være konstruert og kombinert med pliktnormer som begrenser kompetansen ihht visse formelle, materielle, kvantitative eller kvalitative formallogiske betingelser hvor resultatet følger av en analytisk, deduktiv og bindende logisk nødvendighet. Således kan en kompetanse være konstruert og kombinert med de tre pliktmodalitetene forbud, påbud og tillatelser, feks 1) både kompetanse og tillatelse foreligger, 2) kompetanse foreligger, men ikke tillatelse eller 3) tillatelse foreligger, men ikke kompetanse. I en og samme handling kan kompetanse utøves samtidig som en frihet utnyttes eller en plikt følges eller krenkes. Jeg avgrenser mot en nærmere behandling av pliktnormene. Domstolskompetansen kan ev være konstruert og kombinert med avveiningsnormer og retningslinjer som begrenser domstolskompetansen ihht retningslinjer hvor resultatet følger av en avveining av relevante kvalitative argumenter eller prinsipper som verken er strengt deduktive, analytiske eller gir bindende logiske følger, men hvis eventuelle motstrid domstolen mer eller mindre fritt/bundet kvantitativt kan avveie. Jeg avgrenser mot en nærmere behandling avveiningsnormer og retningslinjer.

42 Noen rettssystemer påbyr at domstolen ex officio må undersøke om kompetansebetingelsene foreligger. Påbud kan foreligge om at domstolen skal behandle kompetansekravene på en bestemt kvalitativ måte, eventuelt etter en bestemt rekkefølge av kumulative eller alternative krav og/eller retningslinjepremisser. Om kompetansekravene foreligger, kan domstolen pålegges en plikt til å realitetsavgjøre saken, mens domstolen plikter å avvise saken dersom kompetansekravene ikke er oppfylt.

De juridiske metodene for avgrensning kan være sammensatt av normkomponenter som positivt gir og negativt avgrenser domstolskompetansen.[43]

Reglene om domstolskompetanse tilordner hvor en sivil og kommersiell tvist som har oppstått eller måtte oppstå i et bestemt kontraktsrettsforhold mellom tilbyderen A på T1 og medkontrahenten B på T2 kan eller skal pådømmes.

Den positive avgrensningen tillater A å lokalisere og isolere rettsforholdet med B til et bestemt eller flere bestemte og eventuelt eksklusivt anvendelige rettssystemer.

Den negative avgrensningen egner til å forhindre, ekskludere eller eliminere anvendelsen av (potensielt) konkurrerende rettssystemer.

Således kan A forutbestemme rettsposisjoner ift èn gitt normmengde eller flere gitte normmengder ihht et eller flere lands anvendelige rettssystemer.

a Valg av verneting

Flere rettssystemer tildeler medkontrahentene autonom kompetanse til å velge hvilken eller hvilke domstoler som skal ha eksklusiv kompetanse til å pådømme rettsforhold som har oppstått eller vil oppstå.[44]

Således er enten A alene eller sammen med medkontrahenten blitt gitt autonom kompetanse til ved avtale å tildele en eller flere lands domstoler dømmende kompetanse.

I praksis kan A ensidig bestemme kontraktsbetingelsene ved å tvinge medkontrahenten til enten å akseptere en avtale om valg av verneting eller bli avvist fra å kontrahere og ev. utestengt av en digital sperre (se kap. II, pkt d).[45]

A kan dermed kontrollere de relevante normkomponentene som positivt gir og negativt avgrenser domstolskompetansen. Således kan A velge det forumlandet som tilbyr den mest gunstige løsningen av rettsvalgsregler, prosessuelle regler etc.

---

43 Kontradiksjonsfølgen av positiv kompetansetilordningen er negasjonen negativ kompetanseavgrensning. Kompetansetilordning til lovgivende, dømmende eller utøvende statsmyndigheter hhv gir eller fratar mulighet til ensidig å utøve kompetanse overfor en bestemt krets av subjekter. I det første tilfellet er subjektene avhengige av kompetansen, og kan bli normsubjekter i normen den kompetente statsmyndighet fastsetter, endrer eller opphever. I det andre tilfellet er subjektene uavhengige av kompetansen, og er immune mot statsmyndighetenes fastsettelse, endring eller opphevelse av normer.

44 Feks den norske Straffeloven av 22. mai nr. 10 1902, § 145, annet ledd og § 262. Se også InfoSoc direktivet (Dir. 2001/29/EC). EU tilstreber en harmonisert rettslig beskyttelse mot omgåelse av effektive tekniske foranstaltninger. Den rettslige beskyttelsen av tekniske foranstaltninger berører ikke anvendelsen av eventuelle nasjonale bestemmelser som forbyr privatpersoner å besitte anordninger, produkter eller komponenter til omgåelse av tekniske foranstaltninger, jf direktivets fortale pkt. 49.

45 Vernetingsavtaler kan inntas i en click-wrap avtale eller en egen web-side.

På den ene siden er det universelt anerkjent at vernetingsavtaler bør respekteres så langt som mulig.[46]

På den annen side kan vernetingsavtalen tilsidesettes av gyldighetskrav om materielt innhold og form, og internasjonalt preseptoriske eller eksklusive regler om domstolskompetanse.[47]

Flere rettssystemer kvalifiserer vernetingsavtaler inkorporert i de materielle kontraktsklausulene som en del av den materielle kontrakten hvis innhold og gyldighet skal avgjøres etter de materielle reglene (*lex causae*) utpekt av rettsvalgsreglene.

Betingelsen for å kvalifisere vernetingsavtalen som en gyldig vernetingsavtale varierer blant rettssystemer. Noen rettssystemer krever at avtalen må være avgrenset fra den materielle kontrakten i en selvstendig vedtakelsesprosedyre og at avtalens innhold beviselig må kunne dokumenteres og etterprøves.[48] Her kan et praktisk tidskoordinatsproblem oppstå.

Enten eksponeres B først for den materielle kontrakten. Dersom B vedtar kontrakten, vil B bli eksponert for vernetingsavtalen som B kan vedta eller avvise. Dersom B avviser vernetingsavtalen, får ikke A utnyttet sin autonome kompetanse til å forutbestemme en kompetent domstol. Følgen er at en eventuell kontraktstvist må avgjøres av domstolen som tilordnes kompetanse etter konvensjonelle domstolskompetanseregler.

Eller B eksponeres først for vernetingsavtalen. B kan imidlertid trekke seg fra kontrahering fordi B blir forespurt om å akseptere en vernetingsavtale før B leser den materielle kontrakten. Dersom B likevel vedtar vernetingsavtalen, blir B eksponert for den materielle kontrakten som B enten kan vedta eller avvise.

Det psykologiske spillet mellom tilbud og aksept, og faren for at konvensjonelle domstolskompetanseregler får anvendelse eller at B avviser å kontrahere, kan tale for et tidskoordinatskompromiss der to parallelle (click-wrap) avtaler

46 Jf. resolusjonen vedtatt av INSTITUT DE DROIT INTERNATIONAL, SECOND COMMISSION som 28.08.2003 avholdt en sesjon i Brugge om "The principles for determining when the use of the doctrine of forum non conveniens and anti-suit injunctions is appropriate" punkt E som lyder:"E. It is universally recognized that (subject to special rules based on the policy of the protection of the interests of the weaker party) effect should be given to choice of court agreements in international transactions." Resolusjonen er i helhet inntatt i IPRax 2004, s. 161 f.

47 For eksempel kan partene ihht Brussel- og Luganokonvensjonene Art. 17 og Brussel I forordningen Art 23 gyldig avtale eksklusivt verneting i alle saker bortsett fra saker som faller inn under de obligatoriske og eksklusive vernetingsreglene.

48 Om Brussel- og Luganokonvensjonene, se Gjelsten, Gaute Kr., Formkrav i internasjonale vernetingsavtaler, 1997.

– en for den materielle kontrakten og en for vernetingsavtalen – eksponeres for B simultant,[49] feks i to rubikker eller vinduer på en web-side.

b Valg av leveringssted

Risikoen for at vernetingsavtalen kan bli kjent ugyldig vil tvinge A til å anvende flere juridiske virkemidler for å avgrense handlingsuniverset til et forutbestemt normsystem.

Flere rettssystemer gir og avgrenser domstolskompetansen over kontraktstvister til domstolen på stedet hvor kontrakten enten er inngått eller stedet hvor kontraktsobjektet er levert, enten det beror på faktisk eller avtalt leveringssted.

For å avgrense og velge i hvilket eller hvilke land potensielle søksmål kan eller skal pådømmes, bør kontrakten uttrykkelig inneha en klausul om et avtalt leveringssted (hvor A finner det gunstig å løse potensielle tvister for domstolene).

De fleste rettssystemer gir nærmere betingelser for om og hvilke tilknytningsfaktorer som må foreligge mellom tvisten, partene og domstolsstedet.

IV Når teknisk og juridisk avgrensning er kjent ugyldig eller ikke er anvendt

Ambisjonen om å lokalisere rettsforhold til et forutbestemt normsystem lar seg ikke bestemt realisere dersom vernetingsavtaler og/eller avtale om leveringssted ikke er benyttet eller er kjent ugyldig. Begrunnelsen er at konvensjonelle regler om domstolskompetanse får anvendelse.

Imidlertid kan A til en viss grad kontrollere eller påvirke de relevante normkomponentene som positivt gir og negativt avgrenser domstolskompetansen ved å tilpasse aktivitetene til kompetansereglenes tilknytningsfaktorer.

Digitale, globale overføringer har rokket ved den tradisjonelle oppfatningen om hvilken kontakt eller hvilke tilknytningsfaktorer som må foreligge mellom domstolen og rettsforholdet for å kvalifisere en stats rettssystem som relevant og anvendelig.

Tradisjonelt har tilknytningsfaktorene blitt konstruert etter subjektive, objektive eller fysiske referanseledd. Slike referanseledd, eller stedskoordinater, har vært og er vanskelig å anvende på ulike aspekter og elementer av ytringshandlinger i den digitale transmisjons- og retransmisjonsprosessen.

49 Simultaneksponering er forøvrig vanlig i den konvensjonelle verden.

Flere stater har derfor konstruert nye tilknytningsfaktorer med referanseledd som vektlegger hvor noe skal oppfylles,[50] hvortil noe er sendt eller mot hvor noe rettet,[51] eller hvor noe har hatt en effekt.[52]

Vektleggingen av *hvortil*, men ikke *hvorfra* noe er sendt eller rettet, gir i prinsippet statene kompetanse over all informasjon som er gjort tilgjengelig og potensielt overførbar over Internett.

Få rettsavgjørelser er avsagt. Derfor rår stor usikkerhet om forståelsen av de ulike tilknytningsfaktorene og referanseleddene. Således kan ikke A med sikkerhet kalkulere og forutberegne hva som positivt markerer hvortil informasjonen er/ikke er rettet.

Ambisjonen fremover blir derfor å avklare 1) hvilke faktorer som indikerer eller markerer at kommersielle og profesjonelle aktiviteter foregår i, er rettet til eller avgrenset mot en stat, 2) hvilke faktorer som er rettslig relevante og 3) hvordan de rettslig relevante faktorene skal avveies mot hverandre.

Som det fremgår kan teknisk avgrensningen foregå positivt, negativt eller i en kombinasjon. Avgrensningen kan bestå i å gi/ ikke gi seg selv tilgang til, eller motta/ikke motta henvendelse fra et definert stedskoordinat. Avgrensningen kan foregå på definerte stedskoordinater og til definerte tidskoordinater. Valgene av avgrensningsmåte(r) og steds- og tidskoordinat(er) kan få betydning for ulike aspekter av spørsmålene om internasjonal domstolskompetanse (og rettsvalg).

Noen rettssystemer vektlegger enten ensidig om en aktivitet positivt er rettet mot eller også om en aktivitet negativt er avgrenset fra å bli rettet mot et territorium.

50 Feks Luganokonvensjonen av 16. september 1988, Brusselkonvensjonen av 27. september 1968, Artikkel 5.1 og Brusselforordningen No 44/2001 av 22. desember 2001, Artikkel 5.1.

51 Feks Brussel- og Luganokonvensjonen Artikkel 13(3) og Brusselforordningen Artikkel 15.1(c), annet alternativ.

52 Feks Brussel- og Luganokonvensjonen Artikkel 5.3 og Brusselforordningen Artikkel 5.3.

I amerikansk Høyesterettspraksis er begge metoder relevante, således at amerikanske domstoler avviser å realitetsbehandle rettsforhold når A har gjennomført rimelige tiltak for ikke å etablere kontakt til amerikansk territorium.[53]

EF-domstolen har ennå ikke avklaret om begge metoder er relevante for tolkingen av Brusselforordningen, spesielt artikkel 5.3 og artikkel 15.1c), annet alternativ.[54]

Jeg begrenser meg til peke på enkelte faktorer som kan inneha territorielle markører ved å vise til kap. II, pkt. c.

---

53 Domstolskompetansenormene og begrensningene i amerikansk in personam jurisdiksjonsregler nedfelt i USA´s konstitusjons 14. amendment med tilhørende høyesterettspraksis tilordner domstolskompetanse dersom fire kumulative vilkår er oppfylt. Vilkårene må vurderes i en bestemt rekkefølge: 1) Domstolen må først vurdere om saksøkte har etablert en minimum av kontakt eller tilknytning til forumlandet. 2) Dersom kravet om minimumskontakt er oppfylt, må retten vurdere om saksøkte etablerte kontakten med vilje. 3) Dersom viljeskravet er oppfylt, må domstolen vurdere om saksøkers krav er et krav som har sammenheng med saksøktes minimumskontakt. 4) Dersom kravet til sammenheng er oppfylt må domstolen endelig vurdere om tilordning og utøvelse av domstolskompetanse er rimelig og rettferdig. Forøvrig er rimelighets- og rettferdighetskravet et viktig eksempel på et retningslinjepremiss som enten kan gis form og innhold av en argument- eller prinsippavveining, og som er felles for mange rettssystemer. Totalbedømmelsen av hvilke rettsfakta som kan aller skal ha relevans og avveiningen av hensyn for og mot rimelig og rettferdig domstolskompetanse formuleres av amerikansk Høyesterett tidvis relativt fritt som argumenter for konkret rimelighet og rettferdighet for partene, og tidvis som mer bundne prinsippielle vurderingskriterier som almen rettslig løsning, hvorav noen vektlegger fremtidige konsekvens-, formåls- og nyttebetraktninger, mens andre er mer eller mindre nøytrale eller retroktive i å plassere relevansen av hensyn og avveiningen av disse på tidsaksen. I dette henseende kan prinsippielle vurderingskriterier tjene til fordel for partenes forutberegnelighet.

54 Vedrørende forordningens Art. 15.1c) vektlegger Parlamentet begge metoder, se EP opinion 1st reading Proposal for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM (1999) 348 - C5-0169/1999 - 1999/0154(CNS)) C 146 (2001), p. 94–101. Likeså gjør rapportøren Diana Wallis for the <Commission>{JURI}Committee on Legal Affairs and the Internal Market Opinion of the Economic and Social Committee on the 'Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters', Official Journal C 117, 26/04/2000 s. 6-11. Se også Report on the proposal for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters</Titre> <DocRef>(COM (1999) 348 – C5-0169/1999 – 1999/0154(CNS))</DocRef>, s. 35. Kommisjonen forkastet Parlamentets forslag om også å vektlegge negativ avgrensning fordi "this definition is not desirable as it would generate fresh fragmentation of the market within the European Community", se punkt 2.2.2 i Amended proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (presented by the Commission pursuant to Article 250 (2) of the EC-Treaty)/* COM/2000/0689 final - CNS 99/0154, Official Journal C 062 E , 27/02/2001, p. 243–275.

V Juridisk avgrensning av anvendelig materiell rett

Hittil i fremstillingen har artikkelen fokusert på metoder for å avgrense potensielt konkurrerende rettssystemer ved å avgrense kompetente domstoler.

Naturlig i denne sammenhengen er kort å nevne hvordan avsenderen A kan forutberegne hvilket eller hvilke lands materielle rettsregler (*lex causae*) som skal få anvendelse ved å avtale hvilket lands materielle rettsregler som skal anvendes i tilfelle rettstvist.

Lex causae kan være *lex fori* eller et annet lands lov. Om *lex causae* får fullstendig anvendelse, beror på flere forhold.

Om *lex causae* er *lex fori*, kan internasjonale preseptoriske regler fra et eller flere land som ikke er en del av *lex fori* tilsidesette hele eller deler av *lex fori*.

Om *lex causae* ikke er *lex fori*, kan det samme gjelde. I tillegg kann preseptoriske regler eller regler om *ordre public* i *lex fori* få anvendelse og tilsidesette helt eller delvis *lex causae*.

I denne artikkelen avstår jeg fra en videre behandling av rettsvalgsreglene.[55]

VI Transformering av internasjonal privatrett til internasjonal offentlig rett

Artikkelen har påvist når og hvordan de to pliktmodalitetene påbud og forbud kan sanksjoneres slik at brudd på pliktnormene kan medføre strafferettslig sanksjon.

Flere rettssystemer knytter strafferettslige sanksjoner til handlinger som omgår eller bryter, eller forsøker å omgå eller bryte ulike metoder for interaksjonsavvisning.

Artikkelens puslespill viser at A kan anvende tekniske sperrer for å avvise C som interagerer fra T3 i fasen for geo-lokalisering, selvidentifisering, vernetingsklausul, leveringsstedsklausul og rettsvalgsklausul.

Videre kan A anvende tekniske sperrer som kun tillater B å benytte de overførte digitale tegnene på T2. Følgen er at benyttelse utenfor T2 hindres.

Slike tekniske foranstaltninger avhjelper A{s uforutberegnelighet når vernetingsavtaler og rettsvalgsavtaler er kjent ugyldig eller ikke anvendt.

Således gis A mulighet til å anvende tekniske foranstaltninger for å forhindre eller begrense handlinger som A ikke har gitt tillatelser til.

Jeg skal påpeke to følger av brudd på digitale sperrer.

For det første kan slike pliktbrudd transformere et rent sivilrettslig rettsforhold til også å bli et strafferettslig rettsforhold.

---

55 For en grundig behandling av spørsmålene, se Moss, Giuditta Cordero, International commercial arbitration, Party Autonomy and Mandatory Rules, 1999 (ISBN 82-518-3949-1).

Dermed blir rettsforholdet også kvalifisert som medlem av den internasjonale offentlig rett, herunder strafferett. Strafferetten reguleres av domstollandets interne rett.

I norsk rett nedlegger Grl. § 96 et forbud mot å straffe uten etter lov. Begrepet {lov{ betyr her norsk lov.[56] Følgelig må rettsgrunnlaget for straffbarhet alltid være hjemlet i norsk lov.

Den internasjonale strafferett er en lære om hvor langt nasjonal straffelovgivning rekker og ikke en rettsvalgslære slik som i den internasjonale privatrett.

Som følger blir spørsmålet for norsk retts vedkommende hvor langt den norske straffelovgivning strekker sin virkning. Norsk stafferetts geografiske virkekrets er regulert i Straffeloven av 22. mai nr. 10 1902, første kapittel.

I denne sammenheng vil jeg lansere følgende hypoteser:

- A's strategi for å optimere rettighetskontroll er å gjennomføre de mest effektive og avskrekkende sanksjoner mot omgåelse av de digitale sperrene. Derfor vil A både anlegge sivilrettslig erstatningssøksmål og straffesak med påstand om straff.
- A vil gjennomføre teknisk sperring på T1 dersom straffelovgivningen i denne stat kun har geografiske virkekrets innenfor eget territorium.
- A vil ha større valgmuligheter til å gjennomføre teknisk sperring på T2 og T3 dersom straffelovgivningen i T1 har geografisk virkekrets til handlinger utført på disse territoriene.

For det andre gir flere rettssystemer rettslig grunnlag for at sivile krav som følge av en straffbar handling kan tilordnes domstolen som avgjør straffespørsmålet, forutsatt at denne domstol ifølge sin egen lovgivning er kompetent til å behandle sivile krav.

For eksempel er Brussel- og Luganokonvensjonen samt Brusselforordningen med hjemmel i Artikkel 1.1 anvendelig i "sivile saker" "uansett hva slags domstol saken bringes inn for".

På den ene siden følger av bestemmelsens ordlyd "sivile saker" at straffesaker faller utenfor konvensjonenes og forordningens saklige anvendelsesområde.

På den annen side følger av bestemmelsenes ordlyd at konvensjonene og forordningen likevel er anvendelige på sivile aksessoriske krav pådømt i straffesaker.

Med andre ord knyttes ikke behandlingen av et aksessorisk krav til behandlingen av et hovedkrav.

---

56 Andenæs, Johs., Alminnelig straferett, 4. utgave, 3. opplag, 1999, s. 497 (og se generelt s. 497-527).

Det avgjørende for om aksessoriske krav er omfattet av konvensjonenes og forordningens anvendelsesområde er følgelig hvilket rettsområde det aksessoriske krav henføres til og ikke hvilket rettsområde hovedkravet må henregnes til.[57]

Følgen er at straffedomstolens avgjørelse av det aksessoriske sivile krav kan anerkjennes og fullbyrdes ihht konvensjonene og forordningen.

De fleste europeiske rettssystemer anerkjenner at retten til å kreve kompensasjon for lidt skade påført av en uaktsom straffbar handling er et sivilrettslig krav, hvilket er den underliggende grunnen for Art. 5.4 i Brussel- og Luganokonvensjonen og Brusselforordningen.[58]

Hva som er et sivilt "krav som følge av en straffbar handling" i Brussel- og Luganokonvensjonen Artikkel 5(4)[59] og Brusselforordningen Artikkel 5.4[60] er et tolkingsspørsmål som har avgjørende betydning for omfanget av bestemmelsenes anvendelsesområde.

De fleste europeiske stater hjemler forutsetningen i Artikkel 5.4, men etter varierende utforminger og praktiske betydninger.

I norsk rett bestemmer straffeprossesloven av 1981 § 3 jf kap. 29 hvordan og under hvilke betingelser et sivilt rettsforhold kan kumuleres med et strafferettsforhold.[61]

Straffeprosessloven gir adgang ikke bare for den "fornærmede", men også for "andre skadelidte", som forstås som alle skadelidte, til å kunne få sine borgerlige krav påkjent i forbindelse med straffesaken. Tilbyder A kan feks tilby opphavsrettslig beskyttet materiale skapt av andre enn A selv, og da vil ikke bare A, men også opphavsmennene nyte fordel av Artikkel 5.4 og norsk straffeprosesslov av 1981 § 3 jf kap. 29.

---

57 Louise de Cavel v Jaques de Cavel, Case 120/79, EFD 1980, s. 731, premiss 8 og 9.

58 Følgelig blir det viktig å definere grensen mellom hva som er/ikke er en "sivil sak" ihht Brussel- og Luganokonvensjonen og Brusselforordningen Art 1.1. For Brusselkonvensjonen, se Volker Sonntag v Hans Waidmann, Elisabeth Waidmann and Stefan Waidmann, Case C-172/91, ECR 1993, p. I-01963, premiss 15-19.

59 Se Pålsson, Lennart, Luganokonvensjonen, 1992, s. 95-96, Rognlien, Stein, Luganokonvensjonen norsk kommentarutgave, 1993, s. 151-152.

60 Artikkel 5.4 får anvendelse også når hovedregelen i Artikkel 2 (saksøktes bosted) eller unntaksregelen i Artikkel 5.3 (i saker om erstaning utenfor kontrakt) er anvendelige. Således får Artikkel 5.4 selvstendig betydning når straffesaken pådømmes i et annet konvensjonsland enn den straffetiltaltes bostedsstat etter hovedregelen i Artikkel 2 eller "skadestedet" (det sted der skaden ble voldt eller oppsto) i Artikkel 5.3.

61 Se Andenæs, Johs., Norsk straffeprosess, bind I, 2. utgave, 5. opplag 1999, s. 25-33.

VII Avsluttende kommentarer

1 Målet er ikke fullendt

Artikkelen bidrar til å gi oversikt over tekniske og juridiske metoder for å avgrense interaksjonens potensielt globale tilknytning til bestemte territorier, samt å avgrense suverene staters potensielt konkurrerende rettssystemer.[62] Artikkelen antyder at avgrensningene bør foregå på ulike steder og i ulike, men nære tidsfaser.

Målet har vært å avgrense kolliderende handlingsuniverser til et forutberegnelig handlingsunivers ihht et rettssystem med en gitt mengde rettsnormer hvor motstrid er, eller kan elimineres.

Målet om adekvat reduksjon av mulige verdener er langt fra fullendt og skyldes i hovedsak mangel på adekvate tekniske avgrensningsmetoder,[63] og mangel på globalt uniformerte regler om domstolskompetanse, rettsvalg og tekniske avgrensningsmetoder.[64]

---

62 Artikkelen har utelatt flere spørsmål om og i hvilken grad A kan bestemme over B`s grenseoverskridende utnyttelse av læringsmodulene. Blant annet har jeg utelatt spørsmålet om A i overdragelseskontrakten kan detaljere og kontrollere B`s handlingsunivers for retransmisjon, spredning eller salg av læringsmoduler som inngår i et fysisk gode. Videre har jeg utelatt spørsmålet om A kan bestemme at det er forbudt for B rettslig eller faktisk å disponere over det overdratte kontraktsobjektet slik at det krysser T2`s statsterritorielle grenser (stedskoordinatsbegrensninger). A vil forhindre subrogasjonssøksmål i T3. Derfor vil A forby for eksempel salg fra T2 til T3. Om subrogasjonsspørsmål i intern norsk rett, se Hagstrøm, Viggo, Obligasjonsrett, Oslo 2002 s. 788 flg.; Krüger, Kai, Norsk kontraktsrett, Bergen 1989 s. 841 flg.; Jervell, Stephan: Misligholdskrav mot tidligere salgsledd, i TfR 1994 s. 905 flg. Om subrogasjonssøksmål og anvendelig rett etter Romkonvesjonen, se Pålsson, Lennart, ROMKONVENTIONEN, TILLÄMPLIG LAG FÖR AVTALSFORPLIKTELSER, 1998, s.105. Utelatt er også spørsmålet om tekniske metoder kan begrense geografisk bruk av kontraktsobjektet. Feks har B lastet ned læringsmodulen til sin mobiltelefon. Når B krysser grensen fra statsterritorium T2 til T3, vil B`s mobiltelefon automatisk kobles til T3`s nasjonale telenett. Samtidig kan læringsmodulen programmers til ikke å fungere når B`s mobiltelefon ikke er koblet til T2`s telenett.

63 Det generelle begrepet aksessrettigheter refererer til ulike deontisk automatiserte beslutningsprosesser som gir rett til tilgang til feks et webområde. Herrestad`s doktorgradsavhandling gir betydningsfulle bidrag til hvordan plikter kan uttrykkes, se Herrestad, Henning, Formal Theories of Rights, 1996, spesielt avslutningen i pkt 9.3 som refererer til hele hans fremstilling.

64 Informasjons- og kommunikasjonsprosessen har et visst sirkulært preg. De syv elementene angitt i kap I pkt 2 er gjensidig nødvendige og kausale til hverandre; for uten ytringshandling foreligger ingen informasjon som kan overføres til andre medier. Studier av informasjonen som sådan kan dra fordel av å observere hvordan regulering av et av de sirkulære informasjonselementene vil påvirke de andre, og hvilke direkte, indirekte, faktiske, potensielle, nasjonale og internasjonale effekter reguleringen av et fremfor et annet element vil ha eller kan få i den sirkulære informasjonsprosessen.

2 Hypoteser om det internasjonale søksmålsklima

Jeg avrunder artikkelen med å gi forutsigelser om det internasjonale søksmålsklima sett i lys av mangelen på internasjonale uniforme normer om domstolskompetanse.

For det første kan flere rettssystemers regler om domstolskompetanse positivt og parallellt konkurrere om å tilordne sine respektive domstoler kompetanse til å pådømme tvister mellom de samme parter som har samme gjenstand og grunnlag. På denne bakgrunn kan man gi flere forutsigelser om positive kompetansekonflikter:

- Litispendens regler vil ofte bli påberopt. Reglene forplikter alle andre domstoler enn den hvor saken først er reist til å utsette forhandlingene inntil det er avgjort om den første domstol er kompetent.[65]
- Videre vil den saksøkte part ofte søke å forhindre saksøker fra å anlegge søksmål i utlandet basert på såkalte anti-suit injunctions.[66]
- Endelig vil vi, av ulike taktiske grunner, se en økning av begjæring om midlertidige beføyninger da flere rettssystemer anerkjenner slike begjæringer selv

65 INSTITUT DE DROIT INTERNATIONAL, SECOND COMMISSION, avholdt en sesjon i Brugge 28.08. 2003 om "The principles for determining when the use of the doctrine of forum non conveniens and anti-suit injunctions is appropriate" hvor blant annet følgende resolusjon ble vedtatt i punkt G 3 og 4: G 3: "Parallel litigation in more than one country between the same, or related, parties, in relation to the same, or related, issues, should be discouraged." G 4: "In principle, the court first seised should determine the issues (including the issue whether it has jurisdiction) except (a) when the parties have conferred exclusive jurisdiction on the courts of another country, or (b) where the first seised court is seised in proceedings which are designed (e. g. by an action for a negative declaration) to frustrate proceedings in a second forum which is clearly more appropriate." Resolusjonen er i helhet inntatt i IPRax 2004, 161 f. Se feks Luganokonvensjonen Art 21 som regulerer situasjonen når sak anlegges ved to domstoler som begge er kompetente. Art 21 tar kun stilling til spørsmålet om hvilken av de to domstolene som skal utsette sin avgjørelse og i et gitt fall definitivt erklære seg inkompetent til at påkjenne saken fordi en sak verserer for en domstol i en annen kontraherende stat.

66 INSTITUT DE DROIT INTERNATIONAL, SECOND COMMISSION, vedtok følgende resolusjon i punkt G 5: "Courts which grant anti-suit injunctions should be sensitive to the demands of comity, and in particular should refrain from granting such injunctions in cases other than (a) a breach of a choice of court agreement or arbitration agreement; (b) unreasonable or oppressive conduct by a plaintiff in a foreign jurisdiction; or (c) the protection of their own jurisdiction in such matters as the administration of estates and insolvency".

om utenlandske domstoler er kompetente til å realitetsavgjøre det materielle rettsforhold.[67]

For det andre kan flere rettssystemer negativt og parallelt avvise et og samme rettsforhold på grunnlag av at en domstol i et annet land har bedre forutsetninger til å realitetsavgjøre tvisten, ofte kalt forum non conveniens.[68]

For det tredje kan vi oppleve en økning i strafferettssaker pga strafferettslige sanksjoner for handlinger som omgår eller bryter, eller forsøker å omgå eller bryte ulike tekniske metoder for interaksjonsavvisning (jf kap. VI).

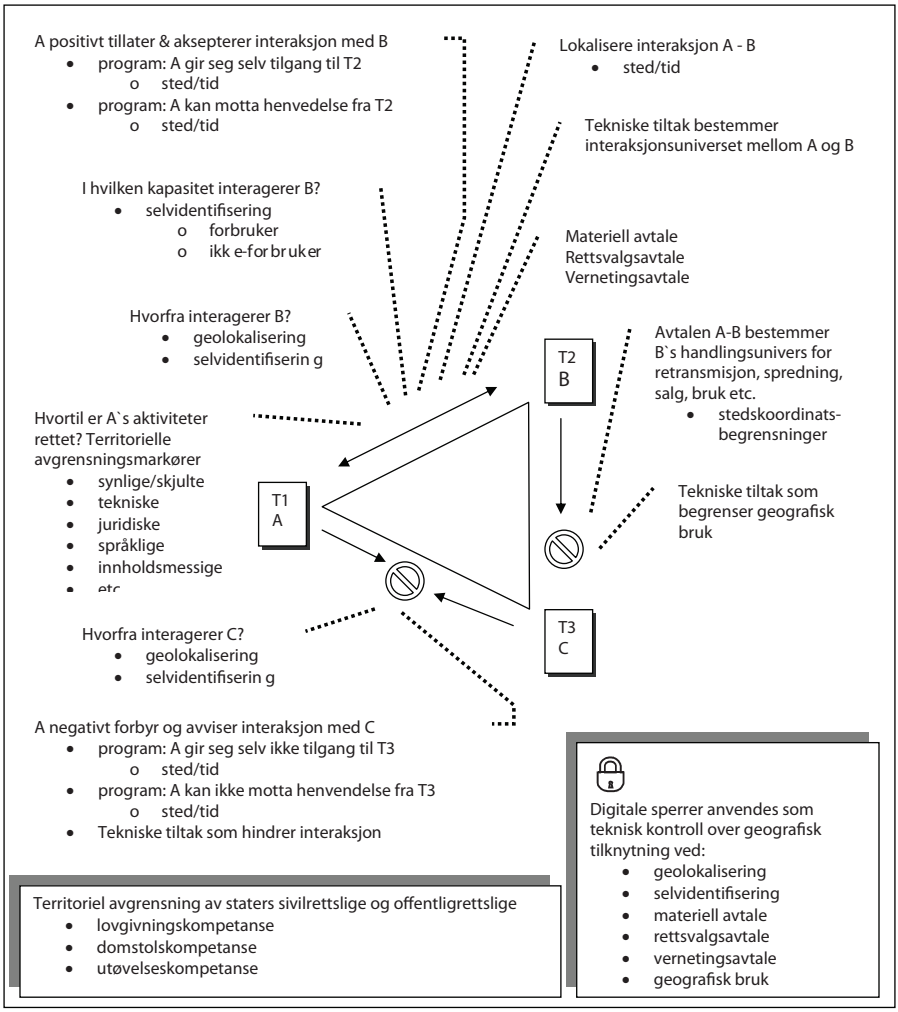
Konsekvensene av mangelen på internasjonale uniforme kompetansenormer, kolliderende handlingsuniverser og det internasjonale søksmålsklima gir liten rettslig forutberegnelighet, økte saksomkostninger pga. parallelle søksmål i flere land eller søksmål i utlandet og uforenlige dommer.

Haag-konferansen avholdt diplomatisk sesjon 14. til 30. juni 2005. Statsdelegatene vedtok det lenge forhandlede utkastet til konvensjon om vernetingsavtaler. Konvensjonen vil først tre i kraft når den er ratifisert av et tilstrekkelig antall land.

---

67 InfoSoc-direktivets fortale pkt 59 bestemmer i denne forbindelse blant annet at "Mellommannens tjenester kan navnlig på det digitale området i stadig stigende grad anvendes av tredjemann til krenkelser. I mange tilfeller er sådanne mellommenn i best stand til å bringe sådanne krenkelser til opphør. Med forbehold av eventuelle andre sanksjoner og rettsmidler, der kan anvendes, bør rettighetshaverne derfor ha mulighet til å nedlegge forbud overfor en mellommann, som overfører en tredjemanns krenkelse av et beskyttet verk eller andre frembringelser i et nettverk. Denne mulighet bør foreligge, uansett om mellommannens handlinger er unntatt i henhold til artikkel 5. Betingelsene og de nærmere bestemmelser for sådanne forbud bør fastsettes i medlemsstatenes nasjonale lovgivning."

68 INSTITUT DE DROIT INTERNATIONAL, SECOND COMMISSION, vedtok følgende resolusjon i punkt G 1 og G2: G 1"When the jurisdiction of the court seised is not founded upon an exclusive choice of court agreement, and where its law enables the court to do so, a court may refuse to assume or exercise jurisdiction in relation to the substance of the claim on the ground that the courts of another country, which have jurisdiction under their law, are clearly more appropriate to determine the issues in question." G 2: "In deciding whether the courts of another country are clearly more appropriate, the court seised may take into account (in particular): (a) the adequacy of the alternative forum; (b) the residence of the parties; (c) the location of the evidence (witnesses and documents) and the procedures for obtaining such evidence; (d) the law applicable to the issues; (e) the effect of applicable limitation or prescription periods; (f) the effectiveness and enforceability of any resulting judgment."


A positivt tillater & aksepterer interaksjon med B
• program: A gir seg selv tilgang til T2
o sted/tid
• program: A kan motta henvedelse fra T2
o sted/tid
Lokalisere interaksjon A - B
• sted/tid
Tekniske tiltak bestemmer interaksjonsuniverset mellom A og B
I hvilken kapasitet interagerer B?
• selvidentifisering
o forbruker
o ikk e-forbruker
Materiell avtale
Rettsvalgsavtale
Vernetingsavtale
Hvorfra interagerer B?
• geolokalisering
• selvidentifiserin g
T2
B
Avtalen A-B bestemmer B`s handlingsunivers for retransmisjon, spredning, salg, bruk etc.
• stedskoordinats-begrensninger
Hvortil er A`s aktiviteter rettet? Territorielle avgrensningsmarkører
• synlige/skjulte
• tekniske
• juridiske
• språklige
• innholdsmessige
• etc
T1
A
Tekniske tiltak som begrenser geografisk bruk
T3
C
Hvorfra interagerer C?
• geolokalisering
• selvidentifiserin g
A negativt forbyr og avviser interaksjon med C
• program: A gir seg selv ikke tilgang til T3
o sted/tid
• program: A kan ikke motta henvendelse fra T3
o sted/tid
• Tekniske tiltak som hindrer interaksjon
Digitale sperrer anvendes som teknisk kontroll over geografisk tilknytning ved:
• geolokalisering
• selvidentifisering
• materiell avtale
• rettsvalgsavtale
• vernetingsavtale
• geografisk bruk
Territoriel avgrensning av staters sivilrettslige og offentligrettslige
• lovgivningskompetanse
• domstolskompetanse
• utøvelseskompetanse