Dag Wiese Schartum og Anne Gunn B. Bekken (red.)

YULEX 2008

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Dag Wiese Schartum og
Anne Gunn B. Bekken (red.)

YULEX 2008

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

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

ISBN 978-82-7226-118-3
ISSN 0806-1912

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

CONTENTS

FORORD

Nå er det jul igjen! – og her julegaven til deg fra medarbeiderne ved Senter for rettsinformatikk og Avdeling for forvaltningsinformatikk. Vi håper og tror du vil finne artikler som er interessante og som kanskje også gir lyst til å holde på og utdype kontakten med vår fagmiljø.

Ved utløpet av 2008 bestod Senter for rettsinformatikk (SERI) av i alt 28 forskere. Blant disse hadde 11 forskere sin primære tilknytning til andre instituttmiljøer ved Det juridiske fakultetet i Oslo, mens 17 tilhører «kjernen» av SERI som er samlet i Domus Nova. De tilknyttede forskerne illustrerer vår rolle som senter, dvs. som et fagmiljø som skal «drive, støtte og integrere forskning, undervisning og formidling i rettsinformatikk og forvaltningsinformatikk» slik det heter i våre vedtekter. Selv om en stor del av vår forskning skjer i fjerde etasje i Domus Nova på St Olavs plass i Oslo, er stedet forskningen skjer på altså ikke avgjørende for at senteret skal fylle sine oppgaver.

Forskningen vår er delt inn i fire områder: Medierett og Internet governance, elektronisk forvaltning, elektronisk handel og personvern og informasjonssikkerhet. I tillegg er spørsmål vedrørende rettsteknologi et tema som gjelder alle forskningsområdene. Ved utløpet av 2008 har vi begynt en innsats for spesielt å satse på nye aktiviteter innen de to først nevnte forskningsområdene. Samtidig er interessen for spørsmål vedrørende personvern og informasjonssikkerhet stor og økende. Denne boken viser litt av bredden i forskningen vår, og peker samtidig mot en rekke nye forskningsspørsmål som vi bør søke svar på i tiden fremover.

God jul og god lesing!

FOREWORD

You have now received this years Christmas present from the researchers at Norwegian Research Center for Computers and Law and Section for eGovernment Studies (SeGoS). We hope you will find this book interesting, and that it will encourage you to maintain and strengthen your ties to the Center and its researchers.

By the end of 2008, Norwegian Research Center for Computers and Law (NRCCL) had a total of 28 researchers. Of these, 11 are primarily connected to other institutes at The Faculty of Law in Oslo. The remainder make up the core team of NRCCL located in Domus Nova. The different locations of our researchers reflect our function as an interdepartmental center. Our charter states that we are a center that «carries out, supports and integrates research, education and dissemination in computers and law and information technology and administrative systems.» Even though a large part of our research takes place in Domus Nova, St. Olavs plass in Oslo; where the research is conducted is not crucial for the research center to accomplish its goals.

The research at the NRCCL can be divided into four main categories: Media Law and Internet Governance, Electronic Government, Electronic Commerce, and Privacy and Data Protection.

In addition; questions concerning the use of legal technology are of importance to all the above mentioned categories.

By the end of 2008 we have initiated new activites within Media Law and Internet Governance and Electronic Government. At the same time the interest in Privacy and Data Protection is on the rise.

This book demonstrates some of the breadth of our research and points at new research areas we wish to delve deeper into in the future.

Merry Christmas and enjoy!

KVEN SKAL TRØYSTE HYPOMONE?*

EIT KAMMERSPEL I TRE AKTER OM VERN AV PASIENTOPPLYSNINGAR

Herbjørn Andresen

Dei som er med:

HIPPOKRATES, *etisk medviten lege*
FREDERICK WINSLOW TAYLOR, *teknokratisk pådrivar*
GEORG APENES, *tilsynsdirektør*
HYPOMONE, *tålmodig pasient*
IMMANUEL KANT, *forteikna moralfilosof*
JEREMY BENTHAM, *forteikna moralfilosof*
DEI REGISTRERTE, *eit vilt kor*

Velkomen til teatret!

Stykket i kveld er eit kammerspel frå mikrokosmos, i tre akter. Handlinga går føre seg i hovudet på forfattaren. Fletta inn blant blødmer og litterært tjuvegods får vi av og til servert ein slags bodskap. Det er ikkje reint lite publikum må bere over med.

Personane fører ein akademisk dialog. Sjangeren er kjent frå gamle meistrar som Platon og Galileo. Ein god dialog er likeverdig, og alle deltakarane uttalar seg med like stor rett. I dei klassiske dialogane lét forfattarane likevel sitt eige syn kome til overflata. I moderne bruk er «dialog» oppfatta som eit snilt og nøytralt verktøy. Ordet smakar av velvilje. Dialogen skal leie oss fram til det felles beste eller til gode kompromiss. I dette stykket er den barokke ytre handlinga eit forsøk på å sleppe laus frå det snille og nøytrale. Den akademiske dialogen er maskert som teater, den sløge planen er å ta dialogen attende som våpen.

Ver vennleg og skru av mobiltelefonen.

---

* Dette skodespelet vart først publisert i tidsskriftet Syn og Segn, nr. 1/2008.

Første akt: Ein innleiande prat i herreklubben

(Tre drygt middelaldrande herrar sit i djupe Chesterfieldstolar rundt eit lågt bord)

Hippokrates: Vyrde herrar. Det er ei sann glede å sjå kva mine etterfølgjarar i legegjerninga får til no i det tjueførste hundreåret. Om eg skal vere heilt oppriktig – slik profesjonen min krev – var det ikkje rare hjelpa mine eigne pasientar fekk. Motiva var dei beste. Min legekunst skulle handle om å vite, eg viste bort overtru og magi. Likevel var mykje i min såkalla vitskap henta frå folketrua. No ser eg til dømes klårt at fire kroppsvæsker som motsvarer fire temperament, var eit slag i lufta. Diagnosar og prognosar vart den gong stilte etter fattig evne. Eg hadde ikkje kjemper å stå på skuldra til.

Apenes: Er ikkje det meir enn naudsynt smålåte av ein som med rette er kalla legekunstens far?

Hippokrates: Jau, og det var no berre ei innleiing før eg slår meg sjølv litt meir på brystet. Det som gjer at eg ikkje raudnar når dei framleis kallar meg legekunstens far, er noko heilt anna enn den pleie mine eigne pasientar fekk. Min eid, som er meir enn to tusen fire hundre år gamal, sørgde for at den øvste plikta for legane i all framtid er å gjere det som høver pasienten best. Nøkkelen til temaet vårt i kveld ligg der. Om vi let vere å tvinge legar til å røpe opplysningar som er gjevne i trumål, vil teieplikta verne pasienten. Får eg tilrå min eigen versjon *(tilgjort høgtideleg)*: «Alt som kjem til mi røynsle under utøving av mitt yrke eller i dagleg samkvem med menneske, som ikkje bør bli kjent for andre, vil eg halde løynt og aldri røpe».

Taylor: Ingen tvil om den einestående posisjonen din som legekunstens far, gamle Hippo. Sjølv driv eg med meir generelle saker. Eg er far til den vitskaplege bedriftsleiinga, og dei rasjonelle teknokratiske framskritt i produserande organisasjonar…

Apenes: Eg er nøydd til å skyte inn noko her. De er jo båe namngjetne gigantar, og eg er sporven i tranedansen. Difor er det noko djupt paradoksalt ved persongalleriet i dette stykket. Trass i at de er gamle, kloke og døde, og trass i tvil om kven som eigentleg skreiv den gamle eiden, og trass i at ein hærskare av dei teknokratane Taylor meiner han representerer, heilt sikkert tek avstand frå han: Eg er den einaste i dette selskapet som er nøydd til å insistere på å få vere ein heilt

ut fiktiv figur. Namnelikskapen med ein nolevande tilsynsdirektør utanfor dette stykket kunne elles ha vorte problematisk. Orsak, Taylor, eg braut deg visst av.

Taylor: Heilt i orden Apenes, eg plar kome til orde før eller seinare. Vi går attende til mitt favoritt-tema. Eg er altså talsmann for eit utbreidd og naudsynt perspektiv på verda. Likevel blir eg ikkje akta og æra på same vis som Hippokrates. Tvert imot. Nær sagt alle som preikar den glade bodskapen sin om organisering, styring og effektivitet, kappast om å ta avstand frå den vitskaplege metoden min. Heilt til det brenn under føtene på leiinga i ei verksemd. Då kjem dei alltid tilbake til min metode, sjølv om dei protesterer på slektskapen og kallar det noko anna. Men eg kjenner att det genetiske materialet mitt – lat meg understreke at det er ein metafor, eg er opphavleg kvekar. Dei som tek avstand frå mi lære, er jo alle mine ekte born: helsesektorens byråkratar, leiinga på sjukehusa, IT-leverandørane… og merkverdig nok ofte dei forskarane som skal forstå helsesystema. Jamvel eg ville ha lika betre om forskarane vågde å fremje ein djupare og farlegare kritikk. Det er pussig å sjå alle dei som utøvar flink og medviten taylorisme, og samstundes tyt og syter om «den menneskelege faktor», eller om at «heilskapen er meir enn summen av delane» og slikt. Eg seier, for å stele eit godt sitat, at «heilskap er eit fåfengt diktarnykke».

Hippokrates: No er det ikkje så underleg at det er viktig for mange å ta avstand frå din metode. Å løyse opp fagleg skjønn og *knowhow* til simple arbeidsoperasjonar undergrev både individuelt ansvar og profesjonell autonomi.

Taylor: Eg løyser ikkje opp *knowhow*, eg gjer han eksplisitt! Min berande idé er ikkje noko anna enn eit klassisk aspekt ved all organisering: Når oppgåvene blir for store eller kompliserte for ein person, blir det naudsynt å hakke opp arbeidet i mindre bitar og setje det saman igjen etterpå. Kva som er den mest rasjonelle måten å dele opp arbeidet på, er i prinsippet berre eit reknestykke. Verktøy og menneske er jamstelte. Først må ein identifisere kvar arbeidsoperasjon, og måle tida den tek, så kan vi sjå nærare på om det er mest rasjonelt å få han utført av ein dyr *high-brow*-arbeidar, av ein billeg proletar, eller av ei maskin.

Apenes: Chaplin fekk poenga frå den vitskaplege bedriftsleiinga di godt fram i filmen *Modern Times*.

Hippokrates: Å dele opp og setje saman igjen oppgåver er du utan tvil namngjeten for. Men er det heilt ærleg at du ønskjer kritiske forskarar, Taylor? Eg får stadig høyre at eg er ein bremsekloss, når eg peiker på at forskinga må ta omsyn til at teieplikta set grenser.

Apenes: Eg blir og stadig kalla bremsekloss. Det er ikkje noko gale med det, kven vil køyre ein bil utan bremsar?

Taylor: De blandar samen to ting. Eg etterlyser meir kontroversielle tema i forskinga. Det er mest det motsette av dykkar ønske om grenser for bruk av pasientopplysningar. Forskingsetiske vaktbikkjer krev altfor ofte at pasienten samtykkjer i bruk av opplysningar berre for å løyse ein rebus i regelverket, og ikkje for å styrkje det reelle vernet av opplysningane.

Apenes: Det du kallar ein rebus, er fundamentale vilkår for å kunne verne noko som helst. Reglane plasserer ansvar hos dei som handsamar opplysningane, stiller krav til relevans, pålegg visse tiltak for trygg handsaming, og gjev pasientane ein rimeleg grad av kontroll og styringsrett. Skal vi endre noko, meiner eg det bør vere å gje pasienten meir kontroll – ikkje mindre.

Taylor: Meir kontroll til pasienten inneber at han får meir å uroe seg for. Det tener ikkje dei vitskaplege framstega. Difor tener det på lengre sikt heller ikkje pasienten. Eg er overtydd om at vi kan verne opplysningane om kvar pasient mykje betre om vi samlar opplysningane i nokre få effektive register. Det gjev full kontroll med bruken av opplysningar, og betre kvalitet i opplysningane. Legane får tilgang til dei opplysningane dei treng. Kvar einskild forskar som får tilgang, treng i dei fleste høve ikkje å vite identiteten på pasientane.

Apenes: Du meiner med andre ord at det er betre for pasienten å vere umedviten enn sjølv å ha kontroll med opplysningane?

Taylor: Eg kan ikkje skjøne anna enn at det er eit mykje betre vern enn å uroe pasientane med å skulle samtykkje. Dersom vi gjev pasienten ein illusjon av kontroll, er den kontrollen likevel berre ein gløtt inn i eiga avmakt. Det er som å gjere den fattige merksam på den klåre retten han har til å kjøpe ein luksusyacht, takka vere den frie marknaden.

Hippokrates: Eg er sjølvsagt samd med Apenes i at reglar om handsaming av opplysningar er naudsynt. Dei mest moderne innanfor profesjonen er til og med opptekne av pasientrettar. Mitt perspektiv i dette spørsmålet er likevel noko annleis. Grunnen til at samtykke må vere hovudregelen for medisinsk forsking, er at all tillit har ei rekkjevidd. Pasienten kjem til ein mann eller kvinne som har fagkunne, stetoskop og kvit frakk, og gjev sine opplysningar i trumål. Problemet for legane er ikkje å halde munnen lukka, men at det er grave

mange lumske hol i teieplikta. Dei skal rapportere hit og dit om det meste, med og utan samtykke frå pasienten. Myndigheitene skal ha sitt, og forskarane skal ha sitt. Legane må til og med gje opplysningar om pasientane vidare til myndigheitene som syter for refusjon – ikkje fordi det gagnar pasienten, men fordi myndigheitene treng å kontrollere om legen krev refusjon på rett grunnlag. Noko liknande skjer òg når apoteka krev refusjon for medisin på blå resept. Om legen ikkje fortel pasienten kor djupe hol det er i teieplikta, bløffar han pasienten. Om han fortel det, kan han skape meir uro enn det som er naudsynt. Ein lege kan i dag sjå alle stader på pasienten, berre ikkje i kvitauget.

Taylor: Aha, så du vil ikkje bli kikka i korta når du skriv krav om refusjon. Ja, ja, sjølv ein lege har vel ei sjuk mor å tale for somme tider. Eg må jo spørje, Hippokrates, du er vel ikkje berre talsmann for utøvande legar med reseptblokk og stetoskop? Din profesjon har jo òg horungar som epidemiologar og andre forskarar. Dei kjem rennande på mi dør som ei oskorei av Nikodemusar om natta. Dei vil ha effektive register å forske på.

Hippokrates: Det seier kanskje mest om ditt sjølvbilete, når du oppfattar dei som vil drøfte ei sak med deg, som Nikodemusar. Men du går som katten rundt den varme grauten. Kva eller kven skal pasienten eigentleg ha tillit til i den vedunderlege nye verda di?

Taylor: Teieplikta som ei dygd for kvar einskild lege var tilstrekkeleg den gong pasienten gjekk til ein einskild lege og fekk all si behandling der. Når legen var ferdig, slo Gud kron og mynt, så gjekk pasienten heim for å leve eller å døy. Slik er det ikkje lenger. Legen er eit hjul i maskineriet, på line med andre menneskelege, organisatoriske, kjemiske og tekniske verktøy. Det gjeld i prinsippet det same for primærhelsetenesta som for sjukehusa. Gud kastar ikkje lenger ein mynt i vêret. Han let dei demokratiske prosessane styre prioriteringane, og demokratiet legg gjennomføringa i handa på teknokratane. Den samla kvaliteten i helsetenesta avgjer om pasienten lever eller døyr. Sett på spissen: Kvar einskild lege er berre meir eller mindre flink til å fylgje føresegner. Pasienten kjem til helsemaskineriet. Pasienten trur seg til maskina!

Hippokrates: Når eg som lege rapporterer opplysningar om pasienten min til eit sentralt register, har sjølvsagt dei andre som får tilgang til opplysningane teieplikt. Problemet er at eg ikkje kan fortelje pasienten kor mange som har tilgang, eller kva opplysningane eigentleg har vore brukt til dei siste fire månadene eller dei siste førti åra. Eg trur ingen andre er i stand til å fortelje det heller. Sjølv om vi godtek at pasienten skal ha tiltru til helsemaskineriet og

ikkje til legen, kan likevel ikkje dette helsemaskineriet godtgjere for pasienten at det er tilliten verdig.

Apenes: Eg vil vere litt nøktern. Det er mogleg å kontrollere bruk av opplysningar i eit sentralt register. Men det er naudsynt med andre åtgjerder enn berre ei teieplikt for profesjonsutøvarane. Taylor burde ta eit klårt ansvar for å gje opplysningane godt nok vern i alle register. Det verker smaklaust og impotent å skyve det ansvaret attende på dei organa som løyver og prioriterer.

Taylor: Dersom lovgjevar vedtek og løyver pengar til det, kan vi organisere inn pasientens kontroll med opplysningar tvers gjennom alle basar og register. Det er eit spørsmål om prioritering. Først må ein kanskje stramme opp, og presisere ein smule, krava til kontroll med handsaminga av opplysningar. Så kan vi setje opp eit reknestykke. Ikkje bli altfor overraska om både legar og mange av pasientane ville velje å lempe noko på krava når dei ser ulike forslag til prioriteringar i samanheng.

Hippokrates: *(smiler ironisk)* Så sanneleg, der fann ordet samanheng sin plass i det teknokratiske paradiset.

Apenes: «Samanheng» tyder jo ofte eit reknestykke med så mange faktorar at det toler storm og ruskevêr frå dei fleste innvendingar og kryssande omsyn. Det er eit stort paradoks å skulle betre personvernet gjennom ein nøktern analyse av faktum, sidan nettopp pasientopplysningar ofte er den innmaten som blir elta og toggen i slike reknestykke.

Andre akt: Vitjande filosofar

Hippokrates: Vi tre kan ha det triveleg med vår rituelle usemje her inne i den faglege faktabobla vår. Alle kjem til orde, og vi kan bruke våre faglege overtydingar og favorittflosklar fritt og uhemma. Samstundes er det vanskeleg å kome vidare, fordi vi eigentleg prøver å samtale om verdispørsmål. Vi treng perspektiv og argument frå det ålmenngyldige, utan å gje heilt slepp på våre faglege posisjonar. Tenk om vi kunne sameine faktasfæren og verdisfæren som to såpeboblar, som forsiktig legg seg inntil kvarandre og deretter smeltar saman til ein større sameina boble.

Taylor: *(ertande)* Det høyrest ut som ein fyrsteleg New Age-cocktail. Merk at eg ikkje brukar ordet svada.

Hippokrates: *(uforstyrra)* New Age kunne jo ha vore ein fin kompliment til meg som levde fleire hundreår føre dykkar tidsrekning, men det var altså ikkje det eg fiska etter. For å seie det med reine ord: Vi treng hjelp. Elles er det ei sak som vi stadig undrast over i min profesjon – at den store bøygen for mange nettopp er å vedgå at dei treng hjelp.

Taylor: Å hente hjelp er ein rasjonell prosess! Eg kan på ståande fot nemne minst fire seniorkonsulentar som kan kunsten å utstyre organisatorisk einsretting med eit høveleg moralfilosofisk teflonbelegg. Orsak at eg kallar ting ved sitt rette namn.

Apenes: Eg deler ikkje det synet at vi tre berre er i stand til å drøfte pasientopplysningar frå ein fagleg vinkel. Vi representerer òg på ulike vis kryssande omsyn og interesser i samfunnet. Ein politisk oppnemnt kommisjon eller noko slikt kunne kanskje gå djupare inn i verdispørsmåla enn det vi gjer her, men konsulentar har eg derimot lita tru på. Dei vil vere for bundne av oppdraget til å ha truverde. Når det er sagt, er eg ikkje prinsipiell motstandar av å hente hjelp. I vår vesle dialog her kunne vi kanskje mane fram eit par av dei gamle moralfilosofane, for å høyre deira meining?

Hippokrates: Dei ville vere ei god hjelp, men som du sikkert forstår, har eg skruplar mot åndemaning. Mitt omdøme som legekunstens far er grunna på at eg avviste magien.

Taylor: Eg ser òg helst at metodane mine for vitskapleg bedriftsleiing ikkje blir kopla med magi og trolldom. Sjølv om mange nasevise og nokre få skarpsindige sjeler av og til peiker på likskapen, er eg redd ei slik kopling vil vere *bad for business*.

Apenes: Då kan eg bere omdømekostnaden med å mane dei fram. Skruplane mine blir sterkt reduserte når det har gått meir enn 60 år etter at dei er døde. *(Han klipper slipset sitt i to strimlar nedanfrå og opp mot knuten, sveivar ein strimmel i kvar hand, og mumlar)*

Gamle heidersmenn
vi treng dykkar vit.
Frå tenkingas eliterenn:
Filosofar, kom hit!

(To trinne, muntre teikneseriefigurar deisar ned i rommet. Den eine har t-skjorte med Immanuel Kant skrive på brystet, den andre har t-skjorte med teksten Jeremy Bentham. Båe har baseballcaps på hovudet, med ein liten plastpropell på toppen.)

Bentham: *High five*, Immanuel! Det er nesten ikkje klokt kor trendy vi to gamlekarar har vorte. Det finst knapt nokon debatt om verdiar eller moral lenger utan at vi blir omtala.

Kant: *(slår si høgre hand mot handa til Bentham oppe i lufta)* Ein ny vår både for det konsekvensetiske og det nytteetiske samstundes. Marknaden for tenestene våre blomstrar, Jeremy.

Hippokrates: Skal dei to førestelle kloke gamlingar? Trøyste oss alle. Vel, eg byrjar med noko enkelt… Vyrde filosofar: Gjer eg rett om eg bløffar pasientane mine til å ha større tiltru til teieplikta enn det er dekning for?

Bentham: *(gjer ein kort piruett)* Pass. Eg er ikkje så god på individuelle variasjonar og spesialtilfelle.

Kant: *(stuper kråke)* For enkelt. Du ville ikkje like å bli bløffa sjølv, difor skal du ikkje bløffe pasienten. Maksimen av di handling må vere noko du ynskjer skal gjelde universelt. Den gylne regelen, eigentleg. *Same shit, new wrapping.*

Taylor: Kortfatta og effektivt. Eg er imponert! Det spørsmålet som valdar meg størst bry, er i kva grad pasienten skal ha rett til å rå over opplysningar som gjeld han sjølv.

Kant: *(står på hovudet medan han svarar)* Same svar som sist frå meg. Du ville sjølv ha føretrekt å rå over dine eigne opplysningar. Ergo er det moralsk rett å gjere det same mogleg for andre.

Bentham: *(står og joggar litt på staden)* Den var vel for billeg, Immanuel. Dersom det hadde kosta det same, og gjeve same resultat for heilskapen, hadde det vore lett å vere samd. Så enkelt er det ikkje. Rettar for pasienten kostar for det første pengar i seg sjølv. For det andre gjev tilfeldige og usystematiske samlingar av pasientopplysningar dårlegare grunnlag for avgjerder om organisering og tenesteyting. For det tredje blir kontrollen med utgiftar til refusjon svakare, og til slutt lir forskinga om datagrunnlaget blir skeivt. For å tale i eit språk som mine dårlege sengekameratar populistane forstår: Mindre råderett

for pasienten sikrar meir helse for kvar krone. Alle må ofre litt, men samstundes tener alle meir enn dei ofrar. *Voilà: L'utilitarisme*.

Kant: Eg kan så vidt hengje litt med i svingane her. Å ofre noko for fellesskapen er jo ei handling som eg kan gjere av fri vilje. Eg kan til og med ynskje at det gjeld som ei universell norm at alle bør ofre litt for eit felles gode. *Scheisse*! Har eg vorte utilitarist?

Bentham: Kategorisk nei, min gode Immanuel. Du er berre litt kledeleg schizofren. Vi to plar jo ha problem med å halde fast ved usemja i konkrete og banale situasjonar. *(Dei held kvarandre i armen og dansar eit par rundar i ring)*

Apenes: Du nemnte forsking, Bentham, som ein av mange grunnar til at kvar og ein må ofre seg litt. I røynda skjer mykje av forskinga etter at pasienten er ute av sjukehuset, og han veit knapt om at opplysningane er rapporterte vidare til ymse register. Det er oftare rett å seie at pasienten er umedviten om bruken av opplysningar, enn å seie at han medverkar friviljug. Kan det høve som god moral å bruke opplysningar utan reelt samtykke, og utan at den same pasienten som er opphav til opplysningane kan få nokon heilt direkte eigen nytte av dei?

Bentham: *(bøyar knea djupt to gonger før han svarar)* Både ja og ja. Det reelle samtykket kan vere noko som ein ofrar både medvite og umedvite. Vi overlet ofte til samfunnet å avgjere kva kvar og ein må ofre. Og: Den størst moglege nytta treng berre å vere ei nytte for flest mogleg menneske. Det er ikkje noko vilkår at den som ofrar seg, inngår sjølv i hopen av dei som har nytte av det. Eg ser at dette kan vere eit farleg grenseland, der utilitarismen kan bli eit skjul for omsynslaus overkøyring av enkeltmenneske. Her blir den demokratiske legitimiteten bak dei val samfunnet gjer, særs viktig.

Kant: *(knipsar lett på propellen oppe på capsen)* Her har eg noko eg må føye til. Eg meiner det ikkje er moralsk rett å sjå eit menneske berre som eit middel. Kvart einskilt menneske skal vere eit mål. Hm. Her gjer eg det vanskeleg for meg sjølv. For forskaren er jo pasienten pr. definisjon eit middel, og ikkje eit mål i seg sjølve. *(Han lyser opp)* Men så er eg i det minste ikkje utilitarist!

Dei registrerte: *(syng unisont, og litt falskt)*

Dei skulle drukne oss i mengda
difor let dei våre identitetar fløtte
Anonymitet held ikkje i lengda
og eit pseudonym kan kanskje rømme
Eit samtykke hindrar oss i å gløyme
men er vi uvitande mistar vi kontroll
Gjenbruk av opplysningar er vond å tøyme
derfor syng vi – dei registrerte – i moll

Bentham og Kant: Å nei. Koret! Det er stikkordet som tyder at vi må av scena. *(Dei løyser seg opp)*

Hippokrates: Kor kom dei frå? Og kvifor kjenner eg eit stikk i samvitet når dei syng?

Apenes: Eg må nok vedkjenne meg at dette mollstemte koret av «dei registrerte» på eit vis er min hjord. Eg er godt kjend med deira dilemma. Dei har rettar, men brukar dei ikkje. Songen lét falskt fordi dei for sjeldan øver saman.

Hippokrates: Dei blei tydelegvis for mykje for våre vitjande filosofar, i alle fall. Min sympati låg hos Kant, men han vakla litt for lett under dei motargumenta som nemnte høge tal og komplekse samanhengar.

Apenes: Ja, eg er heller ikkje sikker på om han heldt heile vegen til Dakar. Men likevel er Kant også min favoritt. Eg er kanskje ikkje heilt uhilda, eg har ein gamal og programforplikta bakfot på Bentham. Han er jo ikkje berre kjend for utilitarismen, han klekte òg ut fengselsarkitekturen «Panoptikon». Ideen er at du frå eit punkt kan sjå alle fangane. Som de skjøner, ser eg ikkje Bentham som noko stort førebilete for personvernet. Likevel er det paradoksalt nok eit markant innslag av hans utilitarisme i det regelverket eg forvaltar. Eg har ofte det privilegium at eg kan velje kampen, men eg får sjeldan velje våpen.

Taylor: Eg overraskar vel ingen om eg seier at Bentham er min mann. Men eg skal likevel vere ærleg nok til å vedgå at den oppvisinga vi fekk, ikkje førte oss nærare eit svar på kven som skal verne pasientopplysningar, på kva måte og i kva grad.

Tredje akt: Herrane spør pasienten

Hippokrates: Det var altså ikkje store hjelpa å få frå moralfilosofane. Kanskje vi skulle gå til det meir radikale skritt å spørje pasienten? Tradisjonelt er jo eg av den oppfatning at vi legar veit best kor kompressen trykkjer. Pasienten skal berre bidra med å fortelje kor det gjer vondt. Men i dette spørsmålet er saka annleis. Det vi eigentleg diskuterer, når all pynt og fjas er skrella vekk, er jo kven som har størst omsut for pasienten. Vi kan spørje han heilt enkelt om kven av oss han trur vil hans beste. Då får vi eit gyldig svar på korleis balansen mellom personvern og helse burde vere.

Taylor: Igjen kan eg samstemme i at dette er ein rasjonell prosess. Dessutan er det vel nærast eit plagiat? Plottet byrjar likne på ei bok som heiter Johannes-pasjonar, der Gud og djevelen prøver å forstå kvinna. Dei let tre Johannes-ar, ein poet, ein professor og ein profet, drøfte saka. Då det viser seg at gubbane ikkje er i stand til stort anna enn å preike om seg sjølv, overlet dei ordet til kvinna. Resultatet blir overraskande. Som sagt, eg er med.

Apenes: Eg kjenner òg til Johannes-pasjonane. Om ikkje eg hugsar feil, var Johann Faust ein av dei tre Johannes-ane. Faust selde jo som kjent sjela si til djevelen, for å oppnå kortsiktige gode. Ein pasient kan vere truande til det same. Det er lett å byte bort kontrollen over eigne opplysningar, og å samtykkje til nær sagt kva som helst, for å bli frisk. Etter at opplysningane er registrerte og spreidde, er det *payback time*.

Hippokrates: Faust, ja. I gamle kjelder vekslar vel førenamnet hans mellom Johann og Georg, om eg hugsar rett?

Apenes: Hm. Då var ballen attende i min famn, eg heiter jo sjølv Georg. Johann og Georg, det blir ein krysning mellom apostel og drakedrepar. Det er jo praktisk tala stillingsinstruksen min. Uansett, i dette stykket vil pasienten vere ein fiktiv person, i likskap med oss. Difor er eg med på notane. Vi spør pasienten! Men korleis finn vi han?

Taylor: Det må vere den enklaste saka i verda. Alle er jo pasientar ein eller annan gong. Vi hentar den første og beste frå salen. *(Han stikk to fingrar i munnen og plystrar høgt og effektivt.)*

Hypomone: Med fare for å verke innbilsk – var det nokon her som plystra på meg? Rett nok er det med å ikkje vilje verke innbilsk berre falsk blygskap. Eg

er ein klisjé, og eg strøyer klisjear rundt meg. Sjølv namnet mitt er ei blødme. Gje meg mine femten minutt. No!

Taylor: Sidan ordet klisjé er nemnt, så var det altså vi gubbane som plystra. Vi vil gjerne ha deg opp på scena. Du har høyrt vår vesle ordstrid. Vil du svare oss, kven meiner du har den største omsuta for deg?

Hypomone: Min første tanke er at det må vere Hippokrates. Det er han eg syner min tillit kvar gong det feilar meg noko. Om eg må ha gips på foten, ei lykkepille, ein bypass-operasjon eller ein dose *placebo forte*, er det han som dekkjer trongen. Eg tiltrur han kjøtt, skjelett og kroppsvæsker. Då er det naturleg å gå frå det som er meir til det som er mindre, og jamvel tiltru han *opplysningar* om meg. Difor blir eg uroa når Hippokrates toar sine hender. Eg forstår at ikkje han sjølv har grave dei djupe hola i teieplikta. Likevel må eg sjå om eg kan finne støtte på anna hold. Det er eit svik om den som eg trur meg til, abdiserer frå ansvaret.

Hippokrates: Eg har ikkje abdisert, eg kjempar ein fagleg og nøktern kamp om *innhaldet* i teieplikta. Det er viktig for meg at pasienten opplever at eg er på hans eller hennar side. Difor må eg vurdere å auke innsatsen. Men, som du sjølv ser, eg har ikkje heile scena her åleine.

Taylor: Vyrde pasient, det er nok meg du kjenner minst frå før. Eg ventar ikkje at du skal ha etablert nokon tillit til meg allereie. Derimot vil eg servere eit par gode argument for at du burde sjå annleis på saka. Helsetenesta blir meir og meir eit velsmurt maskineri. I barske vendingar har eg omtala korleis vi treng dine opplysningar, nærast som mat og næring for dei analytiske og talknusande kjevane som får dette maskineriet til å vekse og bli stadig betre. Resultatet blir at den moderne helsetenesta lukkast i å heve standarden for alle. Ho er eit altruistisk prosjekt. Eg appellerer til det moralske samvitet ditt, og hevdar utan blygsel at mi omsut for pasientane er den beste. Difor skal du tiltru meg dine opplysningar, sjølv om Hippokrates sjølvsagt framleis både snikrar kjøtt og handterar kjemikaliane.

Hypomone: For meg er tiltru til eit abstrakt maskineri ei framand sak. Det er mest så eg høyrer dyreskriket bak. Samvitet mitt kan nok overtale meg til å gje opplysningar for eit felles beste, men berre om eg er medviten og heilt trygg på at føresetnadene ikkje blir brotne. Det må vere eit rimeleg samsvar mellom ulempene for meg og nytta for samfunnet. Dessutan må eg vere trygg på at opplysningane ikkje kan bli misbrukte. Det er mogleg at dette finn sin

plass i helsetenesta i framtida. Men du, min gode Taylor, har nok ein lang veg å gå før tillit til helsemaskineriet ditt kan bli noko meir enn fyllstoff i ein middelmåtig komedie. Du minner meg om han fyren som trår fram frå tåka som ein vandrande skolast. Det er for gale.

Taylor: *(overraskande audmjukt)* Eg skjønar det. Likevel er det ein tanke som bør få modne seg.

Apenes: Til forskjell frå Hippokrates meiner eg at vi ikkje berre kan sjå pasientopplysningar som eit biprodukt av legeverksemda. Opplysningar lever sitt eige liv, det er faktisk det som er grunnlaget for mi oppgåve i samfunnet. Rett grunnlag for å handsame opplysningar, og rette måtar å handsame og sikre dei på, er eigne spesialiserte disiplinar. Det handlar meir om juss og teknologi enn om medisin. Og det er særleg i ei brytingstid som no, når helsetenesta endrar karakter i høgt tempo, at samfunnet treng ein uavhengig kontroll med vernet av opplysningar. Mi omsut for deg som pasient har ein litt annan karakter enn hos Hippokrates og Taylor. Eg tek vare på retten din til å ha kontroll over opplysningane, heilt utan andre omsyn. Korkje det å vere avhengig av legen eller å føle moralsk plikt til å bidra til fellesskapen kjem i vegen når eg er ditt ombod.

Hypomone: Eg ser jo at det kan vere nyttig med eit ombod som kan stå på mi side, anten det er legen eller sjølve helsemaskineriet som handsamar opplysningane mine dårleg. Likevel er eg ikkje overtydd om at du faktisk ville støtte meg når eg treng det mest. Grensene for makta og kapasiteten din er snevre. Det blir for enkelt for deg å vere nøgd med å vinne små sigrar. Det er nyttig for samfunnet, men for meg som einskildpasient blir du eit Flax-lodd – eg må skrape på overflata og berre håpe eg kanskje får noko ut av det. Personvernet blir ikkje godt nok for meg dersom du blir tilfreds med å berre vere eit irriterande sandkorn i helsemaskineriet.

Apenes: Eg forstår uroa. I førre akt vedkjende eg meg Kant som leiestjerne. Det inneber mellom anna at eg ikkje skal bruke nokon som eit middel, men sjå alle menneske som eit mål. Det er kanskje eit høgare ideal enn mandatet mitt gjev meg rom for. Eg kjenner meg diverre treft av at symbolske sigrar kan synast viktigare enn retten til kvar einskild.

Hypomone: *(Talar til salen)* Eg kan ikkje felle nokon eintydig dom. Ingen av dei kan gje meg all omsut. Eg treng både Hippokrates og Apenes. Taylor er eg meir usikker på, men eg kan heller ikkje avskrive han heilt. Kanskje det beste

for meg er om dei ikkje blir samde med det første, men blir sitjande i herreklubben eit par tiår til?

Dei registrerte: *(syng)*

Så rørande at dei alle vil tale vår sak
sjølv om ingen av dei lét oss sleppe fri.
Under sukkerdrasjé har medisinen ein bitter smak
som varar evig i dei registrertes encyklopedi.
No må vi spørje oss om vi har drøymt.
Om hundre år er ingenting gløymt.

Hypomone: Å nei! Koret. Det er mitt stikkord for å forlate scena. *(ho spring ut)*

Taylor: Det var ei nyttig lekse. Eg har kanskje undervurdert pasientane.

Hippokrates: Ja, mine herrar. Det var vel eit godt råd vi fekk. Eg vonar de alle kan bli sitjande her eit par tiår til. Vi har viktige ting å diskutere.

Apenes: Vi sit nok framleis her om tjue år og er danna usamde på det viset ein berre kan vere i djupe chesterfieldstolar. Men på fagleg grunnlag er eg nøydd til å åtvare om at då kan kampen om å verne pasientopplysningar allereie vere tapt.

(Langt borte syng Dei registrerte eit muntert barbershopkomp)

Hypomones stemme: (som ein skjerande dissonans inne frå koret)

Tvi, for servile informantar!
Hu, kva de har rapportert om meg!
Opplysningar blanda frå mange kantar;
stygt er eg elta, profilen min utriveleg.
Hippokrates, kvar har du ført meg?
Eg trudde meg trygg på dine lister.
Taylor har forført deg,
no er eg fanga i hans register!

Teppet går ned. Framfor teppet deisar personane i stykket ned frå lufta, den eine etter den andre. No har alle vorte lubne teikneseriefigurar med rare hattar. Forfattaren trykkjer på knappen til ein applausmaskin. Alle bukkar og tek i mot applaus på boks.

LET THERE BE LITE: A BRIEF HISTORY OF LEGAL INFORMATION RETRIEVAL*

Jon Bing

1 Texts and lawyers

During the First World War, large guns were used by both parties. They were firing without much accuracy. The United States Ballistic Research Laboratories of the ordnance department of the US Army became the leading institution in ballistic science, *ie* the calculations of the trajectories by projeciles fired from the guns. The BRL became located at Aberdeen Proving Ground, Maryland. To calculate the tables was used, among other devices, BRL acquired in the mid 1930's one of the mechanical differential analyzers developed by Vannevar Bush, the scientist who is remembered for convincing Roosevelt in 1941 that the Manhattan project was necessary. By 1943, the analyzers were no longer adequate, and BRL placed an order at the Moore School of Engineering to build a more powerful device, which would become known as ENIAC, the first electronic computer (1945).[1]

This is only to remind the reader of the domains seen as appropriate for computers in the early years. Use of computers for processing natural language texts would be exotic indeed. Computers moved towards business life through accounting (computerising the older alphabetic tabulators for punched cards), and seen as possible tools for any other scheme based on a numeric approach. Among these one found the library classification systems such as Dewy's, and information systems were developed based on the systematic tables, perhaps supplemented by keywords or even brief abstracts. These systems became useful tools for many disciplines. Examples like *Chemical Abstracts,* one of the subject-oriented abstracting services starting in 1907, or the medical Medlars information system (1964), graduating to the on-line version Medline, are examples of systems successfully utilising computer technology to offer an information service.

---

* Much of the historical background until 1994 can be found, though organised in a different form, in Jon Bing et al Handbook of Legal Information Retrieval, North-Holland, Amsterdam 1984, also available at http://www.lovdata.no/litt/index.html. However, I have also relied on personal notes which are not documented elsewhere.

1 Cf Norman Macrae John von Neuman, Pantheon Books, New York 1992:190.

Such schemes seem to rely on there being a distinction between content and text: The chemical process verified may be set out in an abbreviated form without the «information» being lost or necessary distorted. In law, it will often not be possible to make this distinction, «the medium is the message». It is most evident in statutes. The text of a statute is not a vehicle communicating a message from one person («the legislator») to the reader, who may be a lawyer. It is a text constructed after a process usually regulated in great detail. Several persons and institutions may contribute to this text, and the final form of the text may rely on decision processes like voting in parliament. It becomes in principle meaningless to look at the text as a message from one person to another – rather the text is offered as a regulatory instrument, from which one may argue on the existence or detailed content of a rule part of the national legal system, to be backed up by courts and law enforcement agencies. The text has become an object independent of conveying a message between persons; it has become a resource upon itself.

Perhaps this simplistic view may serve to explain why lawyers from the very beginning gave preference to a system which would grant access to the authentic text of the legal sources, the text as formed by the agency within the legal system authorised to issue such sources, like the statutes adopted by parliament, regulations issued by the government, or case law by the decisions of the courts.

In this paper, some attempts will be made to highlight the growth of national legal information systems. The constraints of the length of the paper will make it somewhat episodic or anecdotal, though an attempt has been made to focus on important features of the development, and also by comment indicate what may be of general interest.

2 A retarded child and its impact[2]

In the late 1950s, a bill was passed in the legislature of Pennsylvania. Part of the bill was to change a term in the health law – the phrase «retarded child» should be replaced by the more neutral phrase «exceptional child». This may seem as an example of legislative manicure, but also the amendment indicated a new political attitude to this group of persons, and the political importance should not be underestimated. There are in any jurisdiction examples of such

2 The historical background is set out in Jon Bing et al Handbook of Legal Information Retrieval, North-Holland, Amsterdam 1984, also available at http://www.lovdata.no/litt/index.html.

amendments in the legislation which heralds changes in the policies within a certain area.

Pennsylvania adhered to the principle of regulatory management called «textual replacement». It dictates that any amending regulation must exactly identify which sections and sentences in the existing body of regulations should be amended. One may picture this of the amending regulation containing explicit wording which could be cut out and pasted into the specified parts of the identified existing regulations, giving as a result the new text of each amended regulation. An alternative to this principle is the «omnibus principle», where it is seen as sufficient that an amending regulation contain a section which dictate that all former regulations containing the phrase (or even the rules, which can be specified by different words) – wherever they may occur – are to be deemed amended, without specifying the relevant locations.

However, having the principle of textual replacement, the legislators of Pennsylvania had to identify where the phrase «retarded child» – or a variation of this phrase – actually occurred. This represented a tedious task, and the legislators turned towards the Graduate School of Public Health at the University of Pennsylvania for a solution. Here Professor John F Horty had been working on a manual of hospital law, and had developed indexes to support his work at the Health Law Center. Accepting the contract, Professor Horty set out to solve the problem in the time-tested way of professors: He hired a group of students to read through the legislation and indicate all passages containing the relevant phrase. The result likewise was conventional: The professor found the quality of the work wanting. He hired a new group with an equally depressing result.

It was at this stage he turned towards the Data Processing and Computer Center, which had been established in 1955, and gained co-operation for a more radical approach: Solving the problem using text retrieval. To appreciate the boldness of this approach, one should consider the level of computer technology at this time. For the project, there were available an IBM 650, which was based on vacuum tubes and a drum storage of 2,000 words, and an IBM 7070, which was a transistorised version of the IBM 650, having a magnetic core storage containing 9990 numbers of ten digits each. One may compare the capacity to current examples of information technology, like a digital watch or a pocket calculator. Random access memory units like magnetic disks were not available; data not placed into the central storage units mentioned above, had to be stored on sequential tapes.

In principle, the system Professor Horty developed processed an input text to create two files. One was a «text file», containing the original text with an additional index, which gave an internal address for each element of the text

– like «section 2, paragraph 3 starts at location *n* on the magnetic tape». The other was a «search file»,[3] where all the different words occurring in the text were sorted in alphabetical order, giving for each occurrence the internal address of the word.

The search file could be used as a very extensive index to the text itself: Looking up any term in the search file, the internal address was specified, and the computer system could use this in accessing the index of the text file, and retrieve the word in context from the text file. The user had the impression of searching the «full text»; specifying a word like «child», the system would return with the information that this occurred, for instance, in two sections of the statutory text of the data base. And if the user asked to have these displayed (or rather, printed out), they would be retrieved, using the internal addresses as the key linking the search and text files.

Sorting the words of a text in alphabetic order can be compared, perhaps, to ordering books by authors' names in a book case. Anyone who has ventured to do this will know that new books frequently have authors, whose last names start with a letter early in the alphabet, requiring you to move the books of authors, whose name starts with a letter further into the alphabet, working yourself back towards the place where a space for the new book is needed. This metaphor may give some indication of the practical problems facing the early developers. And, of course, they did not have online systems, but had to deal with batch processing, using punched cards for input and printouts for output.

The system developed by Horty did make it rather facile to identify in which provisions of the Pennsylvania Health Law the word «child» and «retarded» (or grammatical variations of these) co-occurred, and the original contract could be successfully concluded. But it was rather obvious that *any* words in the stored provisions likewise and as easily could be retrieved. It is therefore justified to see this as the first successful text retrieval system, and as such it was demonstrated for an American Bar Association conference 1960. In 1963, the technology was used to build the first computerised legal information service, the LITE[4] system of the Air Force Staff Judge Advocate in Denver, Colorado. The technology also provided the basis for Aspen Systems Corporation, established 1968, which served a large number of states in maintaining their compilations of regulations in force during the early 1970s.

3 Also known as «inverted file» or «concordance».

4 LITE is an acronym for «Legal Information Thru Electronics», and it was launched 13 November 1963 under the inventible slogan Let there be LITE! The service was in 1975 renamed FLITE – «F» for «Federal».

There are many roads to follow from Horty's initiative. In practice, it started the development of computerised legal information services, which today are provided in any jurisdiction, and with major international examples as Reed Elsevier's LEXIS-NEXIS service, or Westlaw and other services of the Thompson Group. But impact on research was also major, and the two major examples are European.

But before leaving the beginning, one may point out that though lawyers are not know for being technological *avant gardists*, text retrieval was actually developed by lawyers and for lawyers, due to the need to consult the authentic text for legal interpretation. The search engines of Internet today harvest what was sown by the early efforts of the legal community.

3 European initiatives

Bryan Niblett was a nuclear research physicist with the UK Atomic Energy Authority.[5] He spent the 1966-67 on sabbatical in California, primarily to learn about computer programming. But as he had been called to the English Bar,[6] he also spent time digging into US research in computers and law. He came across the work of Horty, and planned doing something similar in the UK. On his return, he has already worked out the acronym STATUS (for STATUTe Search), and was determined to develop a machine independent program written in a subset of FORTRAN. Having produced the first version of the program, he run into trouble – the Lord Chancellor advised the UKAEA that to put all the statutes into the system would be an *ultra vires* act, infringing the monopoly of Her Majesty's Stationary Office (HMSO) under Crown Copyright. Therefore, the STATUS system became limited to the atomic energy regulations. It was never impressive as a database; its importance was the program itself and the underlying philosophy of the search language.

It was significant that the program was machine independent, which could be compiled for different computers, FORTRAN being one of the high level languages with acceptable portability. It provided initiatives in other institutions, and a better understanding of retrieval strategies and limitations. On

5 The paragraph is based on private communication from Bryan Niblett to the author.

6 Bryan Niblett therefore combines the two aspects of computers and law – later he became Reader of Law at the University of Kent at Canterbury, going from there to the chair of Professor in Computer Science at Swansea.

this basis, activities were started in Australia, Holland and Norway.[7] The collaborator of Professor Niblett, the former submarine officer Norman Nunn-Price also becomes influential in the development of European legal information services, especially for the European Union.

The other major European example is Colin Tapper.[8] When working at London School of Economics 1961-65, he also became aware of the research by John Horty, and initiated the studies that have become known as «The Oxford Experiments»,[9] as the bulk of the work was conducted after he joined Magdalene College, Oxford (from which he retired as a professor). The value of Tapper's work is not only the very valuable results he provided on the design and performance of retrieval strategies, but also the academic attitude he brought to the field. His major objective was not to get a system up and running, but to understand how text retrieval worked, and how it best could be utilised to access the type of source material which mainly suffered from the shortcomings of paper-based solutions: Case law. Also, he pioneered the work on using case citations for improving performance.

One will note that both these European examples have a certain academic flair. They represent an interest in how text retrieval work, and of the relation between natural language texts and a search language mainly based on Boolean logic. It is justified to observe that the academic interest in text retrieval and computerised legal information services was mainly European. There may be several reasons for this; one probably is that as US services grew commercial, the companies operating the services offered research environments, complete with databases, and challenges which attracted those interests. But for commercial reasons, these environments were less open.

Also Europe had a technological environment less mature than the United States. The computers (many of which at this time were manufactured in Europe) did not perform at the same relatively high level, and were less

7 The Norwegian Research Center for Computers and Law started its NORIS research program in 1970, this was a major effort, for instance LEXIS and West both consulted the NRCCL throughout the 1970s. The research program gave many important theoretical results, but also furnished the basis for the national legal information service, Lawdata, still a successful operation.

8 For a review of his work, see Jon Bing «The policies of legal information services: a perspective of three decades»; Peter Mirfield and Roger Smith (eds) Essays for Colin Tapper, LexisNexis UK, London 2003:147-158.

9 Cf Colin Tapper «Legal Information and Computers: Great Britain», Law and Computer Technology January 1968:18-19. Here is mentioned the «Office for Scientific and Technical Information» at Oxford, which was the name of the framework within Tapper continued his work from LSE. Colin Tapper is well known for his reluctance to have his photograph taken, it therefore with malicious pleasure noted that his portrait appears with the article.

accessible. At the same time, the educational systems for lawyers in many European countries included practise periods which made available well-educated persons for rather trivial tasks. These are two elements which are used to explain the tendency in European systems to rely, to a higher degree than in the United States, on indexes, thesauri, *etc*. Indeed, the first operational computerised system in Europe, the Belgian CREDOC[10] (1967), was wholly based on intellectual indexing. However, CREDOC remained somewhat of an odd example among European systems.

4 The legal information crisis

In Europe, however, another aspect was rather prominent.[11]

In 1970, Professor Spiros Simits published his book *Informationskrise des Rechts und Datenverarbeitung* (Karlsruhe). The main argument in the book is based on the growth of the European welfare states. Turning away from a legal policy where social benefits were awarded based on an assessment of need, the welfare states asserted rights for social security. This implied that decisions became legal in nature, and that an applicant could appeal. The appeal had to be processed according to the legal ideals found in how courts addressed complaints. There was a growth in specialised appeal agencies, like administrative tribunals. Also, in jurisdictions where there was a system of general administrative courts, their case load increased. The appeals should be tried on the basis of the relevant legal sources. Few such sources applied to these cases apart from the prior decisions of the decision-making institution itself. Such sources were not typically included in the traditional legal publications, but were only available through the manual files of the institution. These were cumbersome to search, and consequently the time to process appeals increased.

Admittedly, this is a very crude rendering of the arguments of Simitis, but the point should be clear: There was an acute need to improve the performance of legal research in order to meet the requirements of the modern welfare state. And the solution was available in the form of legal information systems. This was strongly advocated by academic lawyers like Spiros Simitis, Wilhelm Steinmüller and Herbert Fiedler, and the 48th Deutschen Juristentag in 1970 recommended:

10 An acronym for Centre de documentation juridique, the system was established by L'assemble des bâtonniers de Belgique and La fédération des notaires.

11 This is argued in more detail in Jon Bing «Legal information services: some trends and characteristics», Colin Campbell (ed) Data Proecessing and the Law, Sweet & Maxwell, London 1984:29-45.

> *«Die ständige Deputation halt als für dringend geboten, über das Stadium der theoretischen Vorüberlegungen eines Einsatzes datenverarbeitender Maschinen auch für die Rechtspraxis hinaus sic nunmehr am de praktische Verwirklichung, mindestens durch de Schaffung von Datenbanken, zu bemühen, wie dies in Ausland schon weithin geschieht.»*

Already in 1967, the Bundesministerium der Justiz had started planning such a system. This is an amazing example of a systematic approach, living up to the best ideals of German praxis, where the administration was supported by professors like Fiedler, Simitis and Klug, ending up in a major report of 1972 – *Das Juristische Informationssystem – Analysis, Planung, Vorschläge.* On this basis, the JURIS[12] system was implemented, a system still very much alive today. The first services of this system addressed social law (the decisions of Bundessozialgericht) and tax law (the decisions of Bundesfinanzhof), illustrating the point of the need to address the problems of the welfare state.

We will not dwell on the development of JURIS, but note that it was followed by a remarkable academic activity. In the 1970s, Germany by far was the most active country within the area of computers and law. Professor Fiedler headed both Institut für Datenverarbeitung im Rechtswesen at the Gesellschaft für Mathematik und Datenverarbeitung, and Institut für Juristische Informatik at the University of Bonn. At Regensburg, Professor Wilehelm Steinmüller developed his basis for a general theory of computers and law, Professor Fridtjof Haft was active at the University of Tübingen, Professor Wolfgang Kilian established his Institut für Rechtsinformatik in Hannover *etc*. There are several more names that could be added to this impressive catalogue of lawyers taking an active interest in computers and law, developing its many aspects, and contributing to a rich literature.

The German example could be used as an index to what happened in many European countries. I am acutely aware of not being able in this context to even very summarily indicate these developments, but perhaps two more examples may be given.

First, in Italy, a similar pressure towards decisions taken by the administrative courts was felt. Here, the lead was taken by the Corte di Cassazione. Renato Borruso, one of the judges at the court, suggested a system in 1968 based on the traditional *massime* or abstracts of the decisions of the court, and

12 Some confusion may arise from the use of the acronym JURIS also for the US Justice Retrieval and Inquiry System, but the Bundesministerium der Justiz consulted with their American collegues, which agreed to the German use of the name. The US service is now discontinued, see below.

the use of a thesaurus.[13] The design of the system pursued the solutions in more traditional library-type systems, which also made it possible to realise the solution without the massive computer facilities required by the US services. The ITALGIURE-FIND system of the Centro Elettronico di documentazione of the court grew to become an impressive and extensive system under the inspired directorship of Vittorio Novelli, it became a general driving force in Italy with strong policy effects. For instance, a dedicated communication network for ITALGIURE was established between Italian courts..

And there was a broad interest. Vittorio Frosini at the La Sapienza University in Rome had published his *Cibernetica diritto e società*[14] in 1967, in which he emphasised administrative law much stronger than in the Anglo-American literature. In 1969, Mario Losano at the University of Milan[15] coined the term *Iuscibernetica* for the field of *Macchine e modelli cibernetici nel diritto*.[16] The National Research Council established the Istituto per la Documentazione Giuridica[17] in Florence, which engaged in an active strategy of publications and conferences. The Corte di Cassazione started in 1976 a tradition, which was upheld for twenty years, of huge, international conferences spanning the whole width of the expanding area of computers and law, the proceedings published in several volumes.

Second, in France, Professor Pierre Catala at the University of Montpellier in 1965 organised a working group with the objective of developing a legal information service, which in 1967 was formalised as Centre d'études pour le traitement de l'information juridique (IRETIJ). This is – as far as I know – the oldest academic institution within the area of computers and law. It was associated with the problem of accessing the decisions of the appeal courts, which were not subject to any systematic publishing in France. IRETIJ developed a system called JURIDOC, and started documenting appeal court decisions. The system was inspired by the work of Michel Bibent, whose doctoral thesis also probably is the first within the field.[18] It may be fair to say that the efforts, especially after Professor Catala left for Paris, was somewhat drained by the needs of an operational system to the disadvantage of academic research.[19] And in

13 See his review in R Borruso Civita' del computer (2 vol), Ipsoa Informatica, Sesto S Giovanni 1978.

14 Edizioni di Comunità, Milan 1967.

15 He is currently at the University of Piemonte Orientale.

16 Einaudi, Turin 1969.

17 Today this institution is known as L'Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG).

18 L'informatique applique a la jurisprudence, Montpellier 1972.

19 Though Professor Michel Vivant, whose work in substantive information law is prominent, is also from Montpellier, but not working within the sector discussed here.

Paris, there was another working party established in 1967 on the imitative of Lucien Mehl, a conseilleur d'Etat and the grand old man of computers and law in Europe.[20] The Conseil d'Etat also has some functions as an administrative court, and the imitative lead to the establishment of an information service which from 1970 became an independent organisation, Centre de recherches et développement en informatique juridique (CENIJ), which through a series of changing names and mergers with other services has become the current French information service, Legifrance. Though it is somewhat fuzzy, France again offers an example of the needs of the administrative law being a driving force behind the developments rather than the business opportunities which in the United States motivated ventures.

The national development of legal information retrieval will be left at this point. It is unfair to the developments that were to follow– for instance the Swedish Ministry of Justice, which pioneered systems with integrated functions (for instance for printing and retrieval), and the Swedish Law and Informatics Research Institute, which directed by Professor Peter Seipel became so very influential, or to the innovative Vienna system and the work by Robert Svoboda and others in Austria. It is also unfair to those institutions most active within this area today, for instance Professors Jos Dumortier and Marie-Francine Moens at ICRI, Leuwen or the Norma project at the University of Bologna. And it is even more unfair to those whose efforts even have not been mentioned, which include the efforts of my own colleagues at the Norwegian Research Center for Computers and Law and the establishment of the successful national legal information service Lovdata. But there will be other possibilities more fully discuss these aspects.

5 Challenging the legal publishers

The history of legal information retrieval has many aspects, and there may be different views of what many be the more important. But there cannot be any doubt that Ohio is one of the important places to start. At the end of the 1960s, there were numerous attempts of creating information or documentation systems. In 1964, the Ohio Bar Association created a working group for considering the adoption of a computerised system. However, the group concluded that no satisfactory solution was available, and recommended that a new system should be developed. They established a corporation,

20 Mehl is the first known to have contributed a paper on computers and law in Europe, offered to a conference at the Institut techniques des administration publique 21 May 1957, «La Cybernétique et l'administration».

Ohio Bar Automated Research Corporation (OBAR), which contracted Data Corporation of Dayton to look into the problem.

Data Corporation had in 1964 developed a system for the retrieval of Air Force reconnaissance documents. In late 1968, it is told that two neighbours got talking across their fence, one being a partner with Data Corporation and one being the chief executive officer of Mead Corporation, a forest products, paper processing, pulp making company. But the two neighbours saw some possibilities of future synergy, and Mead acquired Data Corporation, including the OBAR project. They brought in Arthur D Little to give advice on restructuring; one of the consultants was Jerry Rubin. The advice was to carve out of the corporation the Information Systems Division, and concentrate on the legal business. In February 1970 this was spun off as Mead Data Central with Jerry Rubin as a vice president.[21]

LEXIS was launched with flair. Jerry Rubin became the front figure; LEXIS established its own high-speed network connection to New York and Washington DC, over time developing into MEADNET. It brings to mind the network established around the ITAGIURE system in Europe more or less at the same time, and though the two front figures – Vittorio Novelli and Jerry Rubin – were very different as persons, they both had a vision, and were able to communicate this vision to others and nurse enthusiasm.

From the beginning, LEXIS had an extravagant feel to it, like the use of colour terminals in 1970. One of the challenges for text retrieval is determining which of the retrieved documents are relevant. Even when a search request is adequate, there will be a certain share of the retrieved documents which are not relevant. These have to be discarded, and it will take too much time to read through the documents in full to make this judgement (though this is finally the test). Therefore, one traditionally adds to the document an abstract, this will provide an efficient strategy for making relevance assessment. But LEXIS did not in its original version have any editorial material, only the authentic text of the cases, regulations *etc*. Writing abstracts would represent a huge investment and long delay. Rather, the user was offered a keyword-in-context (KWIC) format, where the search term was highlighted and displayed with leading and following lines (much like the snippets giving the results of a current search engine). In its 1970 implementation, LEXIS used the colour blue for this highlighting. It was seen as rather extravagant to use an expensive colour monitor only to highlight terms. People literary laughed at

21 Cf Susanne Bjørner and Stephanie C Ardito «An Interview with Richard Giering»; January 2004 Searcher, http://connection.ebscohost.com/content/article/1036116093.html;jsessionid=D0437073C6647A193B3E827575CC0AE2.ehctc1 [17 July 2008]

the Association of Computing Machinery demonstration in New York 1970, Richard Giering remembers.

The establishment of the legal information service LEXIS was a huge operation. There was a historic back-log of cases which had to be entered by key-punching, LEXIS outsourced this to contractors overseas, where the cases were double-punched (to ensure high accuracy) by operators not knowing English. At the same time, new decisions had to be collected at home, which in principle implied a contract with each individual judge. LEXIS brought the approach of a modern computer system to this endeavour; it was also not constricted by a web of traditions. The vision was for the end user to operate the system, not any middleperson or paralegal. Based on this philosophy, LEXIS brought out the UBIQ terminal, a special purpose terminal for lawyers which had the help-text engraved on its keys: Press the key [next case], and the next case would be displayed. The red UBIQ was designed to sit on the desk of a partner in a big law firm.

LEXIS as a commercial system was launched 1973. And at the end of the 1970s, LEXIS announced that all the big law firms of the United States were their clients. By «big law firm» was meant all with more than 100 partners. This very clearly illustrates the difference between the United States and Europe. In Europe, there were in 1980 hardly any law firm with 100 partners, and in many countries there were regulatory restrictions to how large a law firm was permitted to grow.

It is my belief that at this time LEXIS was mainly used as a research tool. The user would have to walk up to the terminal, which typically would be in a library. He or she would type in the search request, and determine which cases might be relevant in a dialog with the system. But he or she would not print out the cases on the cumbersome and noisy line-printer connected to the terminal, which would result in folds of pyjamas-striped printout. Rather, the user would turn to the extensive libraries that any of the large law firms would have. LEXIS had provided the identification of the cases; the books would be collected for the cases to be read and studies in the conventional way. I believe this integration between computer research and extensive libraries is the clue to the success for LEXIS in the 1970s.

LEXIS challenged the largest legal publisher in the United States, West. In 1980, West employed 2,500 persons, among them 150 legal editors, and had a weekly export out of their warehouses in St Paul, Minnesota of approximately 250,000 books. It maintained the national reporter system, and it key index scheme was integrated in the legal system, part of the training of a legal mind. Though starting computerising typesetting in the middle of the 1960s, West had been slow to respond to the possibilities offered by computerised retrieval,

and only when LEXIS had demonstrated that there was a market, West turned towards it.

There were interesting differences between the companies. LEXIS was rather glamorous, sparking of the ideas and the enthusiasm of new technology, while West was encrusted with experience, legal know-how and tradition. LEXIS was based on the programs originally developed by Data Corporation, West found its software across the border.

Since the early 1960s, a treaty project has been going on at Queen's University, Kingston, Ontario. The moving force behind this project was Professor Hugh Lawford, and in 1968 he initiated another project to support his collection and annotation of the treaties of the British Commonwealth, the Queen's University Institute for Computers and Law, which was given the acronym QUIC/LAW. Late in 1968, he had an exchange of letters with IBM or a joint project to explore the possibilities of computerised legal information retrieval. The basis was an in-house IBM program known as INFORM/360 for internal use at the corporate headquarter in Armonk, New York. It is believed that the program was developed to meet the need for litigation support in the major anti-trust proceeding to which IBM was party (and which contributed to the unbundling of software). One of the interesting features of the program was the use of ranking algorithms as alternatives to a plain Boolean query language. Richard von Briesen of QUIC/LAW further developed these into rather sophisticated strategies.

The QUIC/LAW system was from the start conceived as something larger than the Treaty Project of Professor Lawford, it was to be developed into a national legal information service. But the development period was rather stormy, several of the original supporters withdrawing, the Federal Department of Justice conducting a test in 1973. The result was the establishment of a new company, the QL-Systems Ltd with Professor Lawford, von Briesen and Canada Law Books Ltd as the original shareholders.

One of the first ventures of the new QL-systems was to sell their program to West. I believe IBM also used INFORM/360 to develop STAIRS, a general text retrieval systems which became the work-horse for many legal information systems, the first installation probably being the PRODASEN system of Brazil in 1972.

We return therefore to the United States, where West in 1975 launches its own computerised legal information service, the Westlaw, based on the QL-system program. West had many advantages, including it long established relation to the judiciary and the legal community. But West made at least one dubious choice in entering the market, the data base only included the editorial headnotes. The headnotes were written by the editors, and it was believed

that in restricting retrieval to these, retrieval performance would be enhanced. This was a presupposition contrary to known facts; such a document design would impair recall, though it might have a positive effect on precision.

I believe that West looked towards the use of the LEXIS system, where the computerised system was mainly used as a retrieval tool, while the cases were read from the books of the conventional library – books which actually were to a great extent published by West. West believed that by offering a superior tool for researching the headnotes lawyers were used to, they would in the computerised system open their conventional reporter system through a more efficient channel. West did not appreciate that though LEXIS was used as a research tool, the relevance function depended upon the ability to dip into the case at several points. Restricting the access to the headnotes, did in some way «blind» the user.

Therefore, it came as no surprise that West changed its policy in 1978 and included also the authentic text of the cases. Since then, Westlaw and LEXIS have competed in the market with comparable services. The services are different in detail with respect to coverage and features. But the monopoly of West in the paper based world has been broken, there is not a duopoly – and there are many specialised services.

The remarkable success of LEXIS also impressed operators in other markets. LEXIS decided to move into the French market in 1982, and with considerable success, but also with a lesson learned: The whole database had to be converted to a character representation permitting the French accents. LEXIS had then already moved into United Kingdom,[22] and this was to some extent a controversial move. The major English publisher, Butterworth, contracted to co-operate with LEXIS. One of the directors of Butterworth was Professor Colin Tapper, and as he had pioneered computerised systems, one had been waiting for Butterworth to make its move. One might have expected that a joint project with West would be an obvious solution, both companies being legal publishers and perhaps with a somewhat similar culture. The co-operation with LEXIS therefore came rather unexpected. I have learned that Butterworth in fact approached West and suggested a joint venture, but was turned down – West would not take any interest in activities outside its home jurisdictions.

In the UK market, the European Law Centre Ltd had taken an initiative in 1979 for a computerised service with one of the originators of the STATUS program, Norman Nunn-Price, as its director. The EUROLEX effort had a

22 This decision was announced at the 1978 conference of the British Society of Computers and Law.

European perspective, and in 1981 a new and more aggressive phase was initiated with David Worlock as head of the organisation. The major legal publisher Sweet and Maxwell made an exclusive agreement with EUROLEX in 1982, which also made an agreement with Westlaw for making US material available to European users. EUROLEX was acquired by the Canadian based international publisher Thompson, and the competition between LEXIS and EUROLEX in the UK market became fierce, but brief. Legal policy arguments favoured EUROLEX, which was a «national» company compared to the LEXIS service, which actually was serviced also for its UK customers out of its facilities in Dayton, Ohio. But overnight the EUROLEX service was closed down by Thompson, as the CEO David Worlock was told about this one hour before the rest of the company. It really brought home that legal information services no longer was something academics or enthusiasts fiddled around with in their spare time, it had become part of the more ruthless world of business.

The international publishing industry has now taken over both the US major services. Reed Elsevier owns LEXIS, and Butterworth is also part of that company. West – which for a long time remained a family company – has been taken over by Thompson, which has interests in a large number of legal information services throughout the world.

6 The vision receding

In understanding the early developments in Europe, it is also necessary to appreciate the role played by a small number of institutions. These forged the persons working with legal information services into a rather close-knit community, helped to communicate test results and experiences in an informal way, and played a large part in reciprocal political support for the policies adopted.

First, the Council of Europe played an essential role in the early developments. On the initiative of the «Committee of Experts on the Publication of state practices in the field of public international law», a «Committee of experts on the harmonisation of the means of programming legal data into computers» started its work in 1969. I believe no one will be offended by me saying that longish name of the committee reveals that it was formed without a clear understanding of its objective or the means to achieve such an objective. And the committee changed its name to the more acceptable «Committee on Legal Data Processing» in 1974.[23] For the rest of the century, this Committee

23 Formally, this was a new committee succeeding the former. I served as a chair for this committee 1981-82.

was a central forum for an exchange of ideas and experiences with respect to computers and law. The substantive law was not part of the area for this committee – but it explored legal information services and justice administrative systems as well as teaching in the area of computers and law. Members of the Committee were a mixture of bureaucrats, policy makers and academics – and there would be annual international meetings with rather ambitious programs. Often the success of international committees is measured in the number of legal instruments adopted – the Committee certainly adopted such instruments,[24] but its main achievement was the communication it facilitated between European institutions, not only at the meetings of the Committee itself, but at the annual international events, which was organised in different member countries. Around the Committee grew a loose-knit community of experts within public administration and universities with a strong, though informal, communication.

It is not possible to understand the co-ordinated development of legal information services in the different European jurisdictions without awareness of the exchanges taking place through the network built by this Committee. The Committee also strongly supported academic activity, not least through the adoption of recommendations of making introduction to computerised systems a compulsory part of legal education, and suggesting a curriculum in the teaching of computers and law.

One may see the Committee on Legal Data Processing as the pivot of a wheel with many spokes. Mention has already been made of the congresses of the Corte Suprema di Cassazione, which attracted large audiences. There were also considerable activity and conferences centred around the Istituto per da Documentazione Giurdica in Florence, and the enthusiasm of the Italian legal community embraced the whole of Europe, inviting them to join the march towards the future of law. In the United Kingdom, the British Society for Computers and Law[25] was founded; its meetings were also of an international nature and included barristers and solicitors as well as lawyers within government – all excited about legal information retrieval and how to bring its advantages to the UK (which by no means should prove easy).

In Germany there were formed societies, which still are very much active, of the same nature, and which addressed policy issues with considerable heat. These meetings perhaps did not contribute as much to the general international discussion – as German was the conference language, this tended to exclude

24 An example is R(83)3 on the «protection of users» of legal information services.

25 The Society was founded 11 December 1973 based on an initiative of the Scottish Legal Computer Research Trust, which itself was founded in January 1970.

a wider international audience, but it has an integrating effect on the German language areas of Europe.

The main point of this small paragraph is to convey the feeling of enthusiasm and comradeship which was developed at this time – from the early 1970s and onwards to 1990. The European development cannot really by understood without considering this swell of common purpose – carrying us, it was believed, towards national, integrated – and probably monolithic – information services.

This was not realised. The obvious reason was the introduction of the PC and office automation. For the vision of the one, integrated national information service was to a large extent the shadow of the available architecture for computer systems: Mainframes with terminal networks. When office automation was introduced, this did not in the first years stimulate communication. Even the establishment of a local area network was not without its problems. The philosophy lead to the development of rather isolated islands, the PC on your desktop might be linked to some local resources like a printer – but not to central files like a national information system. When the CD-ROM was introduced in 1984, systems based on this became popular. Though the storage capacity of a CD-ROM seemed large compared to other media at this time, it was obviously insufficient for a truly national information systems. It was more suitable for sector-oriented systems, for instance tax law. But CD-ROMs were well suited for publishing and management of rights according to the same model as for books, which – it may be argued – made publishers more interested in the field, an interest which carried over into the next phase, as already indicated above

For the next phase came – communication was sorted out, LANs were linked into wider area networks. And then – at the beginning of the 1990s – the control of Internet was relaxed, permitting other institutions than those related to research having access to this international infrastructure. Nearly at the same time, World Wide Web was realised within Internet, web browsers became available and content could be reached from your desktop computer. This was the time when Content was crowned as King – computer technology had matured sufficiently to make vast libraries of text, images and sound available.

But again this did not bring back the vision of the integrated, national legal information services. There may be several reasons for this, but one certainly was that as the threshold of publishing material on the web was lowered, many institutions wanted their own home page and to make their own material available through this page rather than supply the material to some central facility.

7 A changed technical context resulting in new legal policies

As the threshold for publishing went down, new parties took an interest in the legal material. The new environment hungered for contents. A possibility was to convert existing material for re-utilisation on the web. This strategy had the attractive advantage that a lot of material could be made available in a short time. But there usually would be formalities to be met before such material could be uploaded, an obvious formality – which usually also cost money – was clearing the copyrights associated with the material.

However, in the United States copyright was not claimed in the primary, legal sources like statutes, regulations and case law.[26] Therefore, such material was available to furnish a basis for new services supplementing the established services or challenging them in the market place.

One of the United States systems was JURIS (an acronym for «Justice retrieval and inquiry system»), developed in the early 1970s to serve the attorneys of the Department of Justice. In launching the service, it was emphasised that «minimal standards of due process and equal protection of law» were to be extended to all citizen, and that «fulfilment of these requirements depends on timely access to reliable and up-to-date information».[27]

The major objective of JURIS was to make available the legal material generated within the department itself – we recognise this need from the origin to the European systems discussed above. In addition, JURIS was given from FLITE the total text of the United States Code. And since 1982, under a contractual arrangement with West, JURIS received weekly updates of case law for its federal and digest files which otherwise was only available through the commercial Westlaw service.

Unlike the «raw» legal sources, the West material was subject to copyright, at least the material created by their editorial staff, like the headnotes. West

26 It is not quite clear how the doctrine of Crown Copyright applies to the different jurisdictions of the United States. It is reported that in 1984, Crown Copyright was used as a basis for state legislation in New York restricting the sale of data from the Legal Retrieval Service of the Bill Drafting Commission of the state legislature to competing services. But this is an exception; in general copyright in primary legal sources is not claimed. Cf «The policies of legal information services: a perspective of three decades», in Peter Mirfield and Roger Smith (eds) Essays for Colin Tapper, LexisNexis UK, London 2003:153.

27 George R Kondos «Introduction to JURIS – Justice retrieval and inquiry system», Abidjan World Conference on World Peace through Law, 1973.

had also successfully claimed copyright in the pagination system[28] and other elements. The contractual arrangement with the Department of Justice was designed to avoid third parties through JURIS gaining access to Westlaw material and in this way avoiding paying fees or in other ways circumventing the policies of West.

The Department of Justice as a federal agency falls within the scope of the freedom of information legislation. Carole D Hafner, herself a major figure in the history of legal information retrieval,[29] requested in 1991 samples of legislative texts from JURIS for research in computational linguistics. The request was denied. Public interest groups such as the Taxpayers Asset Project (TAP), National Technical Information Services (NTIS) and the American Association of Law Libraries (AALL) queried West on its willingness to make its database available to public access. In a press release of 30 September 1993 West announced that it would not seek renewal of the contract with the Department of Justice. The Clinton administration announced that the National Science Foundation would fund a project to enhance future access to government information. This announcement was made on a Friday, the following Monday the administration announced the permanent shut-down of JURIS from 1 January 1994.

The story is highlighted by the decision of the US District Court of Columbia.[30] After it had become known that the JURIS service would be discontinued, the information service Tax Analysts requested access to parts of the database containing West material. The court concurred with the Department of Justice, and held that «the West-provided data in JURIS is not an 'agency record' under [Freedom of Information Act] and this Court lacks jurisdiction to compel Defendant [Department of Justice] to disclose the information sought by Plaintiff».

---

28 LEXIS was paying US$ 50,000 annual in license fees to West for incorporating the pagination system, based on West Pub Co v Mead Data Cent., Inc, 616 F Supp. 1571 (D. Minn. 1985), aff'd, 799 F 2d 1219 (8th Cir), cert denied, 479 US 1070 (1986). In a subsequent case, Matthew Bender and HyperLaw v West (SDNY 94-Civ 0589, 19 May 1997, United States District Court) Judge John Martin determined that West could not claim copyright in its enhanced versions of decisions as included in its reporters. However, Matthew Bender was acquired by Reed Elsevier in 1998; therefore the decisions were not pursued. It is doubtful whether the copyright in the pagination system would be upheld according to the Supreme Court's interpretation of the copyright originality test in Feist Publications, Inc, v Rural Telephone Service Co, 499 US 340 (1991).

29 Carole D Hafner An information retrieval system based on a computer model of legal knowledge, UMI Research Press, Ann Arbor 1981.

30 TAX ANALYSTS, Plaintiff, v. UNITED STATES DEPARTMENT OF JUSTICE, Defendant, and WEST PUBLISHING COMPANY, Defendant-Intervenor, 913 F Supp. 599.

The example of JURIS demonstrates some of the explosive policy power of the web technology, blowing away part of the older infrastructure designed and determined by technological circumstances. The exclusive arrangement between the department and West was discontinued – at least in this respect – and the money which used to go into the maintenance of JURIS would partly be used to purchase legal information services from West or LEXIS in the market place. At the same time, the court decided that a legal source was not an «agency record», and therefore not subject to the freedom of information legislation.

8 The Legal Information Institutes

Another major example of the new possibilities stimulating new initiatives is provided by the Legal Information Institutes.

In 1992, the LII of Cornell Law School[31] was launched by Peter Martin and Tom Bruce, co-directors. «The legal information industry in the U.S. in the mid-'90s had focused totally on judges and lawyers and hadn't paid attention to the information needs of others,» Peter Martin has stated. «One of our powerful early discoveries was how much demand outside those professional sectors there was – ordinary citizens trying to make sense of laws that impinge on their lives[32] … The Cornell LII offers the United States Code, an organised compilation of current federal laws; and the collections of all recent opinions of the US Supreme Court and New York State Court of Appeals … Making information accessible on the web in a manageable format has been a challenge – there are 13 US Circuit Courts, each putting its decisions on the web. The problem is that data structures and formats differ from site to site: researchers need some solution, for instance a search engine that reaches across those structures.»

The Cornell Law School LII may have been the first service of its kind on the Web,[33] and a Legal Information Institute has become a generic term indicated a certain type of operation on the Web.[34] There are namesakes as far-flung as New Zealand, Zambia and Kazakhstan.

---

31 Cf http://www.law.cornell.edu/.

32 Cf Linda Myers «CU Law institute web site has latest legal information, from Miranda to Elian», http://www.news.cornell.edu/Chronicle/00/4.27.00/Legal_Info_Inst.html [25 July 2002].

33 One will appreciate that 1992 is very early indeed for such a service.

34 The term «Legal information Institute» (LII) refers to a provider of legal information that is independent of government, and provides free access on a non-profit basis to multiple sources of essential legal information, cf Graham Greenleaf, Philip Chung and Andrew Mowbray «Free access to law via Internet as a condition of the rule of law in Asian societies: HKLII and WorldLII», http://www2.austlii.edu.au/~graham/publications/2002/HKLII_WorldLII_Jan02/HKLII_WorldLII.html#Heading3 [25 July 2002].

It may not be unfair to maintain that the LII represent a reaction to a protective attitude towards legal material. Though in most jurisdictions excluded from copyright as permitted under the Berne Convention art 2(4), there remain exclusive arrangements designed to harvest profit from making the material available. But rather to be protective, the material should be made available for as low cost as possible to whoever want to build a value-added service on this basis. For instance, this is the policy underlying the EU re-utilisation directive.[35] It may further be argued that the LIIs have been most successful – and most needed – in jurisdictions where the legal material has been formally controlled, like in the countries applying the Crown Copyright doctrine, or something similar.[36]

One of the more remarkable LIIs, is the Australasian Legal Information Institute (AustLII), jointly established by the University of New South Wales and the University of Technology, Sydney with Professor Graham Greenleaf and Professor Andrew Mowbray taking the initiative in 1995. This is an effort with an impressive ambition, and a background in the policies of legal information services in Australia, where the doctrine of «Crown Copyright» prevails. AustLII is based on the belief that it is in the public interest that authorities should aim to maximise access to the «public legal information» that they control. AustLII argues that unless governments and agencies positively co-operate with non-commercial bodies by providing them with raw data in computerised form, non-commercial bodies are unlikely ever to be able to publish the data in any form.[37]

There are several characteristics of the AustLII that make the service remarkable – the scope of the data base is one thing, the programs developed to enhance the service, and support search strategies is another. But perhaps most important are the standards AustLII sets itself for making legal sources available in a complete and authentic form, a service to integrate material and to be trusted.[38]

35 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

36 One may refer to the experience of Niblett when trying to introduce a statutory information service. In general, see Stephen John Saxby Public Policy and Legal Regulation of the Information Market in the Digital Network Environment, CompLex 2/1996, Norwegian Research Center for Computers and Law, Oslo.

37 Graham Greenleaf, Andrew Mowbray, Geoffrey King and Peter van Dijk «Public access to law via internet: the Australasian Legal Information Institute», http://www.austlii.edu.au/austlii/articles/libs_paper.html#RTFToC11 [25 July 2002].

38 Also other LIIs have similar standards, for Cornell LII see Thomas R Bruce «Some Thoughts on the Constitution of Public Legal Information Providers», http://www4.law.cornell.edu/working-papers/open/bruce/warwick.html [26. July 2002].

AustLII has also many offspring, one of them being the WorldLII, a co-operation between itself and British and Irish Legal Information Institute (BAILII). AustLII has taken upon itself to attempt creating a truly international information resource; not only are the materials made available by the LIIs listed under WorldLII, but a search engine has been developed to index legal sites around the world. There is a toolbar available for most browsers, and lawyers should download this – it will provide an on-screen visual evidence of future possibilities.

The enthusiasm for the LIIs should not obscure some important policy tensions. The needs of the professional user of legal sources requires an efficient research tool. Certainly, the public should be given as easy access as possible to statutes and other important legal material. But use of the authentic legal sources is not trivial. There may be – and in my mind I am convinced there are – different requirements for a service catering for the public and a service meeting the requirements of the professionals. And I am not at all certain that the specialised tools needed by a rather small number of professionals should be paid for by the public at large.

The services offered by the LIIs are often buffered by the policy of *publication legis* and a reference to the basic right of all citizens to know the law. This justification is *not* challenged. But it is challenged that it is wise, or even possible, to satisfy *both* the needs of the lay user *and* the needs of the professional user by the same information service. Even though much of the authentic material would be identical, the user requirements for a friendly service does differ. The tension between these two objectives can be discerned in several aspects of services from LIIs. For instance, Cornell LII integrates it services with legal education, and AustLII has several features to help lay users.[39] And for the professional user we would like to see further developments, for instance more sophisticated ways in presenting search results, better integration with in-house services (for instance for litigation support) *etc*.

9 The vision upgraded

Above, with a certain *tristesse,* it was observed that the vision of a consolidated national information service had been disrupted by the advance in information technology, first introducing office automation, and then web services. Of

39 One of the innovative features of AustLII is an expert system integrated in the information service, when the user has identified a provision in a statute, the user may (where available) switch to an expert system mode that will guide the user through a series of questions in order to advice the user whether the provision will apply to the problem of the user

course, the vision never was realistic. A jurisdiction is too complex, there are too many possible perspectives that they could or should be contained within one system. The only way to ensure objectivity and a sufficient diversity is to support several systems.

The limiting factor may be the economical constraints within a jurisdiction. We have seen how a large market like the United States may support several large scale and general legal information services like LEXIS and Westlaw. In other jurisdictions, there may be a need for the public sector to provide the necessary economic basis for a national service.

Because legal information services are not only a question about the market, it is also a question of what services have to be available for ensuring due process and the other ideal policies of a society ruled by law. In a national perspective, one should be sensitive to requirements and restrictions.

But there is also a need to look towards an international solution. We need to find possibilities of exploiting the advantage of other jurisdictions having legal material which may be of interest. Current principles of using material across frontiers have been forged in a situation where it has been difficult to exploit case law or legislative reviews from other countries. Today, there are regional legal systems where it would make good sense to access decisions and other material from other countries. The European Union may serve as an example, regulations and directives are issued for a large number of jurisdictions, and it would be useful if the material generated by courts and other institutions in applying these provisions was available for the other countries within the union. There are examples of services offering such solutions, like CaseLex[40] reporting on Supreme Court decisions relating to European legal instruments.

But these attempts are still in the making. We should be guided by the vision of WorldLII, and look for knowledge based solutions which seek out and consolidate material on request of the professional user. And computational linguistics seem to have progressed sufficiently to offer the user the possibility to have the material rendered in a language he or she may understand, at least sufficiently to determine whether that material may be relevant.

If this is realised, we will see that the dynamics of the legal system itself, where a legal argument take into consideration prior decisions, may over time work itself into a more harmonised view as courts and other institutions puzzle together not only the pieces of their national systems, but also try to make them fit with a bigger, international picture.

40 Cf http://www.caselex.com/.

BESKYTTELSEN MOT OVERVÅKING I DEN FYSISKE OG ELEKTRONISKE VERDEN*

Inger Marie Sunde

Referatet viser at betegnelsen «overvåking» benyttes om kontrolltiltak av svært ulik art, og at det ikke kan tas som utgangspunkt at alt som kalles overvåking, virkelig setter personvern og rettssikkerheten på spill. Det anføres at EMK gir utilstrekkelig vern mot overvåking, noe som illustreres av utviklingen i bruk av åpen fjernsynsovervåking. Dessuten representerer den teknologiske utvikling i seg selv en vesentlig utfordring for rettssikkerheten, hvilket gir behov for å oppstille spesielle notoritetskrav, for eksempel for bruk av dataavlesing. Til slutt reises det spørsmål ved legitimiteten av strategisk overvåking for å verne om samfunnssikkerheten. Konklusjonen er at de politiske ambisjoner om å sikre personvernet bør ligge på et høyere nivå enn EMK krever.

1 Alle er mot overvåking, men ingen vet hva det er

Hvis man spør hvem i en gruppe som er for, og hvem som er mot, overvåking, vil nok de fleste vil si at de er imot, men de vil samtidig ha problemer med å si hva overvåking er. *Første tese er derfor at fordi ingen egentlig vet hva overvåking er, vet ingen hva de er imot.*

Spørsmålet om man er for eller mot overvåking, er dessuten urimelig, fordi det alminnelige utgangspunkt er at selv om overvåking er negativt i seg selv, må vi tåle det, dersom formålet i tilstrekkelig grad er rettferdiggjort. Hva vi har oppe til vurdering er således om overvåking kan godtas gitt de interesser som står på spill. Interessene forutsettes å være hensynene til rettssikkerhet og integritetsbeskyttelse (personvern), og i siste instans, betingelsene for et fritt og demokratisk samfunn. I overvåkingsdebatten bringer man derfor gjerne opp dilemmaer av typen; skal vi ofre personvernet for å avverge terror, eller skal vi beholde personvernet mot å tåle en viss risiko for å bli drept?

I det følgende skal vi se på om det er mulig å utlede en felles forståelse av ordet «overvåking», og deretter drøfte om det foreligger et tilstrekkelig vern mot overvåking.

---

* Artikkelen er tidligere publisert i «Forhandlingerne ved Det 38. nordiske Juristmøde i København 21.-23.august 2008, s. 457–479»

2 Noen bruksmåter av ordet «overvåking»

2.1 Overvåking: Et spørsmål om kontroll

Rent språklig betyr overvåking å følge med på noe; dvs. en aktivitet som kan være både harmløs og ønskelig. Det er imidlertid unaturlig å bruke overvåking, f.eks. om at elevene følger med på undervisningen. Årsaken er at overvåking pr definisjon har et kontrollformål, og således innebærer et maktperspektiv. Vi er derfor med på et eksempel om at fjernsynsovervåking i klasserommene benyttes for å kontrollere om elevene følger med på undervisningen, men ikke på at elevene overvåker læreren i undervisningssituasjonen.

I sin kjerne handler overvåking om utøvelse av kontroll ved bruk av observasjon, registrering, varslingsrutiner og informasjonsanalyse. *Observasjon*, ved å lytte eller se, ved menneskelig sansebruk eller tekniske metoder, må anses som et grunnvilkår for å tale om overvåking. De øvrige elementene kan foreligge i tillegg, men vil ikke bestandig være tilstede.

Iblant fremholdes det at fordi formålet med overvåking både kan være omsorg og kontroll, er begrepet tvetydig, noe som gjør det vanskelig å bestemme nettopp hva man er kritisk til.[1] Språklig utledes tvetydigheten fra det engelske ordet «surveillance», som har sin rot i fransk «sur veille» (over + se), og derigjennom til latin «vigilare» (holde øye med). Norsk og dansk språk inneholder to beslektede uttrykk, nemlig «overvåke/-våge» og «våke/våge over». Omsorgsaspektet knytter seg til det sistnevnte uttrykket, for eksempel «moren som våker over sitt syke barn». I det moderne velferdssamfunnet kan statens omsorgsoppgaver fungere som begrunnelse for den overvåking som, for eksempel, etablering av et sentralt reseptregister med opplysninger om borgernes medikamenthistorikk og utskrivende lege, sies å representere. Et viktig formål er imidlertid å holde kontroll med medikamentutskriving, så kontrollaspektet er fremtredende. Overvåking som tiltak for ivaretakelse av samfunnssikkerheten, anses å være begrunnet i et kaldt kontrollbehov; overvåkingen skal hindre vold og uorden. Men, som man skjønner, også dette formålet har en omsorgsdimensjon, nemlig å skape et sikkert samfunn til borgenes beste.

Eksemplene viser at det kommer lite ut av å foreta en distinksjon mellom omsorg og kontroll i relasjon til overvåking. Mens kontroll bestandig vil være en del av begrunnelsen for overvåking, vil omsorgshensynet i større eller mindre grad kunne gjøre seg gjeldende i tillegg. Bevisstgjøring av omsorgsdimensjonen viser imidlertid at overvåking ikke nødvendigvis henger sammen med

1 Lyon (2005) s. 3.

onde regimers styresett, som for eksempel Orwells storebrorsamfunn, med sin timelige gjenpart i etterkrigstidens totalitære regimer.

2.2 Overvåking i lovgivningen

Ordet «overvåking» er ikke legaldefinert i norsk rett og kan knapt anses som noe rettslig begrep. Når ordet forekommer i lovgivningen, er det ofte i forbindelse med objekter eller fenomener som ikke umiddelbart reiser spørsmål med hensyn til personvern og rettssikkerhet. For eksempel benytter norsk lovgivning ordet «overvåking» om å holde oppsikt med territoriet, miljøet på Svalbard, epidemier, gjennomføring av EØS-forpliktelsene, offentlig regulering av ervervsvirksomhet, datatrafikk og økonomiske transaksjoner.[2]

Hvis vi skal vurdere om overvåking i for stor grad går på bekostning av rettssikkerhet og integritetsbeskyttelse, er det selvsagt først og fremst tiltak rettet mot *person* som påkaller interessen. Bestemmelser som eksplisitt omhandler overvåking mot person er det imidlertid få av. Overfor Forsvarets etterretningstjeneste gjelder et *forbud* mot å *«overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer»*.[3] Videre finnes det regler om *«fjernsynsovervåking»* i personopplysningsloven og straffeprosessloven. Åpen fjernsynsovervåking av offentlig sted eller på sted hvor en begrenset krets av personer ferdes jevnlig, kan både politiet og private foreta. Overvåkingen er meldepliktig til Datatilsynet og skal tydelig skiltes og varsles.[4] Skjult fjernsynsovervåking har bare politiet kompetanse til å foreta, og formålet må være *etterforsking,* eller som ledd i etterforsking *å avverge* en straffbar handling.[5] Politiets sikkerhetstjeneste (PST) kan benytte metoden også for rent *forebyggende* formål.[6]

---

2 Lovene i den rekkefølge de er nevnt i teksten, er riksgrenseloven (lov 14. juli 1950 nr. 2) se § 1; Svalbardmiljøloven (lov 79/2001) se § 62; smittevernloven (lov 55/1994) se § 3–7; EFTAs overvåkingsorgan (nå ESA – EFTA Surveillance Agency) er nevnt i en rekke lover, f. eks. betalingssystemloven (lov 95/1999), råoljeloven (lov 54/1999) og årsregnskapsloven (lov 56/1998); referanse til organer som har til oppgave å overvåke offentlig regulering av ervervsvirksomhet er inntatt i flere lover, f. eks. konkurranseloven (lov 12/2004) se § 24, og verdipapirloven (lov 19/1997) se § 12–2a. Til slutt skal det refereres til ehandelsloven (lov 35/2003) § 19, og til hvitvaskingsloven (lov 41/2003) § 15.

3 Lov om etterretningstjenesten § 4 (lov 11/1998).

4 Personopplysningsloven (lov 31/2000). Reglene om fjernsynsovervåking står i kapittel VII §§ 36–41, og legaldefinisjonen av «fjernsynsovervåking» i § 36, inneholder ordet «personovervåking».

5 Straffeprosessloven (lov 25/1981) § 202a og § 222d.

6 Politiloven § 17d (lov 53/1995).

I vår sammenheng er også de nevnte reglene om overvåking av *datatrafikk* og *økonomiske transaksjoner*, relevante, når opplysningene som samles inn i medhold av reglene, sier noe om enkeltindividers handlinger.

Forsåvidt gjelder *datatrafikk*, er det nærliggende å reise spørsmål om registreringsplikten som følger av *datalagringsdirektivet* representerer overvåking.[7] Direktivet pålegger tjenesteyterne en generell lagringsplikt for abonnements- og trafikkdata. Formålet er å sikre data som kan nyttes til å avdekke, etterforske og strafforfølge kriminalitet. Lagringsperioden skal være minimum 6 måneder og maksimum 2 år. Lagringsplikten gjelder ikke kommunikasjonens innhold. Direktivet inneholder imidlertid ikke ordet «overvåking», noe som er egnet til å overraske siden det i samfunnsdebatten er beskyldt for å lede til omfattende overvåking uten historisk sidestykke. Direktivet taler utelukkende om *datalagring* («*data retention*»). I skrivende stund er ikke direktivet gjennomført i norsk rett, men slik direktivteksten foreligger har lovgiver knapt foranledning til å benytte ordet «overvåking» i de nasjonale reglene. Danmark innførte lagringsplikt (1 år) i forbindelse med den «første terrorpakke» i 2002, jf. retsplejeloven (rpl.) § 786 stk. 4. Reglene benytter ikke ordet overvåking.[8]

Forøvrig inneholder ehandelsdirektivet art. 15, et forbud mot å pålegge tjenesteyterne av overførings- og lagringstjenester «en generell plikt til å overvåke den informasjonen de overfører eller lagrer eller en generell plikt til aktivt å søke etter fakta eller forhold som tyder på ulovlig virksomhet».[9]

Bestemmelsen er til hinder for et generelt overvåkingspåbud, men ikke for å pålegge tjenesteyter plikt til å overvåke *spesielle deler* av datatrafikken, f.eks. målrettet kontrollvirksomhet for å avdekke barnepornografi. Men fordi man ikke på forhånd vet hvilken tjeneste som eventuelt misbrukes, krever også målrettet deteksjon og varsling en *generell kontroll* av datatrafikken. Spørsmålet er om art. 15 er til hinder for slik kontrollvirksomhet.

Et springende punkt er om «å overvåke» er en referanse til menneskelig kunnskap (hos tjenesteyter) om ulovlig virksomhet, eller om det også omfatter rent automatiserte deteksjonsprosesser. Hvis det sistnevnte er tilfelle representerer forbudet en meget stor restriksjon, som indirekte også rammer målrettete tiltak for å avdekke kriminalitet.

I norsk rett er forbudet gjennomført nokså ordrett, uten særlig veiledning i forarbeidene, og det er synd å si at regelen er klar.[10]

---

7 Direktiv 2006/24/EC.

8 Reglene er utdypet i den omfattende logningsbekendtgørelsen, jf. VEJ nr. 74 af 28. september 2006.

9 Direktiv 2000/31/EF.

10 Ehandelsloven § 19; Ot.prp. nr. 4 (2003–2004).

Overvåkingsforpliktelsen som påhviler *finansinstitusjonene*, går ut på at de må ta i bruk *elektroniske overvåkingssystemer* som skal *«muliggjøre oppdagelse av og rapportering av mistenkelige transaksjoner»*.[11] Selve rapporteringsplikten som ble innført i 1994, er ansett som et vesentlig fremskritt i bekjempelsen av økonomisk kriminalitet, herunder av hvitvasking og korrupsjon. Plikten til å ta i bruk elektroniske overvåkingssystemer (innført i 2003) skal effektivisere rapporteringsplikten gjennom automatiserte funksjoner for deteksjon og varsling av mistenkelige transaksjoner.[12] Reglene er utslag av et utstrakt internasjonalt samarbeid.[13]

Det hersker altså to motsatte prinsipper for regulering av *tjenesteyteres* overvåking for å avdekke kriminalitet. Mens finansnæringen pålegges en generell overvåkingsplikt, er utgangspunktet det motsatte for ekombransjen, selv om det foregår ulovlig virksomhet.

2.3 Overvåking i politiets begrepsbruk

Politiets metodebruk er grunnleggende sett basert på innhenting, lagring og bruk av opplysninger om andre. Formålet er å sørge for ro og orden, og å avverge og forfølge kriminalitet, herunder terror og terrorrelaterte handlinger. Bak informasjonsinnhentingen ligger kontrollformål, og svært mye av politiets virksomhet kan derfor kalles overvåking.

I forbindelse med de senere års utvidelser av straffeprosessuelle metoder til bekjempelse av terrorisme og annen alvorlig kriminalitet, har man i Norge beskjeftiget seg med begrepsbruken knyttet til politiets metoder. Politimetodeutvalget reserverte således overvåkingsbegrepet for *«politiets generelle observasjoner rettet mot allmennheten, når det ikke foreligger konkret mistanke om at det er begått eller forberedt noen straffbar handling»*.[14]

Overvåking skal dermed avgrenses mot *målrettede inngrep* basert på mistanke om at en straffbar handling er begått, typisk bruk av tvangsmidler som teknisk sporing, kommunikasjonskontroll, romavlytting og dataavlesing. Overvåking skal også avgrenses mot generelle observasjoner rettet mot allmennheten som foretas av *andre enn politiet*. Tjenesteyternes lagring av kommunikasjonsdata, finansinstitusjonenes kontroll for å avdekke mistenkelige

11 Plikten er hjemlet i hvitvaskingsloven § 15 (lov 41/2003). Den siterte begrunnelsen står i Ot.prp. nr. 72 (2002–2003) pkt. 7.5.

12 Rapporteringsplikten var opprinnelig hjemlet i hvitvaskingsforskriften av 7. februar 1994 nr. 118, gitt med hjemmel i finansieringsvirksomhetsloven (lov 40/1988). Reglene ble i 2003 flyttet til hvitvaskingsloven, med hvitvaskingsforskrift av 10. desember 2003 nr. 1487.

13 Se beskrivelse av de folkerettslige forpliktelsene i Ot.prp. nr. 72 (2002–2003) pkt. 2.

14 NOU 2004:6 Mellom effektivitet og personvern pkt. 7.2.3 s. 57.

transaksjoner og privat iverksettelse av fjernsynsovervåking, er således *ikke* overvåking etter politiets begrepsbruk. Dette står i en viss kontrast til begrepsbruken i den alminnelige debatt og i lovverket.

I Danmark går det relevante skillet mellom tiltak som representerer et inngrep overfor borgeren og som derfor krever lovhjemmel (for eksempel straffeprosessuelle tvangsmidler), og tiltak som ikke representerer noe inngrep, de såkalte *overvågningsmidlerne* (for eksempel patruljering, åpen fjernsynsovervåking og registrering).[15]

Politiets begrepsbruk synes å forutsette at overvåking omfattes av den alminnelige handlefrihet. Dermed blir det paradoksalt å reise spørsmålet om det hersker et tilstrekkelig vern mot overvåking.

2.4 Samfunnsfaglig bruk av ordet overvåking

Innenfor samfunnsvitenskapen har man arbeidet mye med å forstå og karakterisere overvåking som fenomen, og fagdisiplinen er i realiteten storprodusent av argumenter mot overvåking. Den rettslige diskurs er ikke lukket for disse argumentene, så jurister kan ha nytte av å vite hva samfunnsvitenskapen mener med overvåking.

I *«A Report on the Surveillance Society»* fra 2006, samlet en rekke overvåkingseksperter seg om en beskrivelse av fenomenet, slik det arter seg i dag.[16] Ekspertutvalget innledet med en mild kritikk av sin oppdragsgiver, sjefen i det britiske datatilsynet, som i et intervju i 2004, hadde advart mot at *«we are sleepwalking into a surveillance society»*. Etter ekspertenes syn var denne advarselen lite relevant fordi overvåkingssamfunnet for lengst er en realitet. Det er faktisk slik at det moderne samfunnet er tuftet på overvåking, som følgelig ikke kan avskaffes uten store økonomiske og sosiale konsekvenser.

Overvåking er fremfor alt et produkt av det moderne velferdssamfunnet, forårsaket av teknologiutvikling, byråkrati, effektivitetskrav og markedskrefter. I mangel av effektive motkrefter, lar ikke utviklingen seg stanse (her råder determinismen), med mindre drastiske mottiltak settes inn. Det innebærer i så fall at vi må avstå fra goder vi har vennet oss til og finner naturlige (for eksempel å motta tilbud via nettet, eller få effektiv medisinsk hjelp på grunnlag av et sentralt pasientregister). En strategi basert på teknologiske løsninger for å fremme anonymitet (kalt PETs, dvs. *Privacy Enhancing Technologies*) anses ikke som tilstrekkelig for å sikre personvernet; i stedet må systemer som kan utnyttes for overvåkingsformål, avvikles. Et hovedbudskap er dessuten at bruk

15 Henricson (2007) s. 142.
16 Wood/Ball (2006).

av overvåking sender et signal om at man ikke stoler på den som observeres, dvs. at overvåking underminerer sosiale strukturer for tillit.

På et punkt faller den samfunnsfaglige bruken av overvåking sammen med den rettslige, ved at overvåking fremfor alt handler om å samle inn og utnytte personopplysninger («dataveillance»). Men ellers er den samfunnsfaglige forståelsen mye videre; for det første ved at overvåking anses som nødvendige mekanismer i det moderne samfunnets struktur. For det annet anses mange flere aktører enn myndighetene å forestå overvåking, og da i særdeleshet private foretak som utnytter persondata i kommersiell virksomhet. Kort sagt: Håndtering av persondata anses som overvåking.

2.5 Oppsummering

Gjennomgangen har vist et betydelig sprik i bruken av ordet overvåking, men en rimelig oppsummering synes å være at det er tale om *utøvelse av kontroll ved bruk av personopplysninger*. Innenfor denne kjernebetydningen kan det sondres mellom forskjellige overvåkingsformer avhengig av (i) overvåkingsgrunnlaget, dvs. om det skjer på generelt grunnlag eller på grunnlag av konkret mistanke; (ii) hvorvidt overvåkingen skjer åpent eller skjult; (iii) hvem som forestår overvåking; (iv) hva som skjer med opplysningene, for eksempel om de lagres eller ei.

Et spørsmål som melder seg er om en diskusjon om overvåking er *identisk* med en diskusjon om personvern. Hvis så er tilfelle handler debatten i realiteten om den generelle håndteringen av personopplysninger, men da blir overvåking som tema uten selvstendig interesse. Samfunnsvitenskapens overvåkingsdiskurs later til å basere seg på en slik begrepsforståelse, noe som synes å ha liten analytisk verdi, men kan ha en viss retorisk effekt.

Med tanke på den rettslige drøftelsen i det følgende, presiseres det at overvåking benyttes om kontrolltiltak som involverer bruk av personopplysninger, og som iverksettes av hensyn til nasjonal sikkerhet eller for å forebygge eller oppklare kriminalitet. Det er primært kontrolltiltak iverksatt av myndighetene som faller innenfor dette overvåkingsbegrepet.

Et annet spørsmål er om overvåking bare bør benyttes om såkalte *strategiske metoder,* dvs. kontroll og informasjonsanalyse uten konkret mistanke, eller om det også bør omfatte politiets *målrettede mistankebaserte metodebruk*. Jeg synes en vid begrepsbruk er hensiktsmessig, og inkluderer også den sistnevnte metodebruken, når det er tale om hemmelige metoder. Begrunnelsen

er at slike metoder reiser spesielle rettssikkerhetsspørsmål, samtidig som de utfordrer personvernet.

3 Eksempler på hva som ikke er overvåking

Det kan være grunn til å konkretisere den negative avgrensningen av overvåkingsbegrepet, med noen eksempler som går igjen i debatten. Eksemplene underbygger *tesen om at overvåkingsspørsmål ofte forveksles med andre spørsmål.*

3.1 Kontroll uten bruk av personopplysninger

For det første har vi *sikkerhetskontrollen på flyplasser*, en kontroll som er blitt vesentlig skjerpet som følge av den økte terrorfaren, og som derfor har en klar kobling til myndighetenes trusselvurdering og sikkerhetspolitikk. Datatilsynet har gått til felts mot sikkerhetskontrollen og fremholdt at den representerer en form for overvåking som svekker personvernet, fordi den bryter med et prinsipp om at kontroll bare bør utøves på grunnlag av konkret mistanke. Kontrollen påstås å krenke den tillit som grunnleggende sett bør herske mennesker imellom, og å støte an mot «uskyldspresumsjonen» («en grunnleggende tese i en rettsstat»),[17] og bør derfor såvidt forstås, avvikles.

Denne argumentasjonen gjør ikke noe forsøk på å forklare hvordan en akseptabel og effektiv kontroll alternativt skulle kunne foregå, og det er vanskelig å se at Datatilsynet fyller sin oppgave som vakthund for personvernet, ved å bringe opp dette eksemplet.

Det kan være vel så nærliggende å vurdere sikkerhetskontrollen i et *kontraktsrettslig perspektiv.* Fra passasjerens ståsted er det tale om at man har betalt for en reise, og da under den selvsagte forutsetning at det er en sikker reise. Erfaring har vist at flykapring er en reell risiko, og sikkerhetstiltak må følgelig anvendes. Det forutsetter en generell kontroll av passasjerene, og for å få sikkerhet må den enkelte samtykke til også selv å bli kontrollert. Rettslig sett kunne man tenke seg at flyselskapet ble ansett for å være i kontraktsmessig mislighold med hensyn til sine sikkerhetsmessige forpliktelser, dersom ombordstigning skulle skje etter Datatilsynets prinsipper.

Andre eksempler i samme kategori er sikkerhetskontroll ved inngang til institusjoner med store verdier, f.eks. muséer, og til arenaer med store publikumsansamlinger (f. eks. fotballstadion). Slik kontroll synes å ha lite med overvåking å gjøre.

17 Slettemark (2006). Merk referansen til tillitsargumentet i overvåkingsrapporten nevnt i punkt 2.4.

3.2 Generelle tiltak med målrettet varsling

Videre har vi *generelle overvåkingsmetoder* som kun registrerer kontrollrelevant atferd. Fotobokser langs veiene er et slikt eksempel, og er så kontroversielt i Norge at det ble drøftet i Politimetodeutvalgets utredning.[18] Til tross for at metoden er generell (alle bilistene må passere fotoboksen), gir den bare utslag dersom bilisten bryter loven ved å kjøre for fort. Registreringen av persondata skjer altså målrettet og for et legitimt formål (styrke trafikksikkerheten). Når det i tillegg er gitt tydelige varsler om fotoboksene langs veiene, synes heller ikke dette tiltaket å påkalle synderlig interesse i en overvåkingsdebatt.

En slik kontrollform kan imidlertid fremkalle motforestillinger av annen art, dvs. hva slags samfunn ønsker vi å ha? Bør myndighetene praktisere nulltoleranse også overfor småfeil, bare fordi teknologien har gjort det mulig? Et rimelig svar er at her foreligger et politisk handlingsrom og velgerne må ta ansvar for å stemme inn politikere med de «rette» verdiene. Hvis det ikke er mulig har vi et politisk, snarere enn et rettslig problem.

En metode av lignende karakter er tyverimerking av varer i butikkene; alle varer er merket, men bare de som blir stjålet gir utslag på detektoren.

3.3 Generell lagring av elektroniske kommunikasjonsdata

Til forskjell fra fotoboksene innebærer *pliktig lagring av kommunikasjonsdata* at *alle* oppkoblinger til det elektroniske kommunikasjonsnettet, det være seg på telefoni- eller internettsiden, skal registreres og lagres. Plikten påhviler tjenesteyteren, noe som gjør det nødvendig å begrunne hvorfor tiltaket skulle anses som overvåking. Begrunnelsen måtte være at lagringen er pålagt av myndighetene, på grunn av behovet for slike data til å bekjempe terror og alvorlig organisert kriminalitet.[19] Dermed er det av underordnet betydning at lagringen rent faktisk skjer hos tjenesteyter.

Men igjen, la oss se på hva som skjer: Dataene skal oppbevares konfidensielt som persondata og bare utleveres til politiet i forbindelse med avdekking og forfølgning av straffbart forhold. Senest etter 2 år skal dataene slettes. Det synes derfor som om vi først og fremst står overfor personvernspørsmål, som handler om sikkerheten for at dataene blir behandlet etter personopplysningsregelverket, et spørsmål som er relevant for de fleste næringsdrivende.[20] Det at elektroniske tjenesteytere som andre næringsdrivende, håndterer persondata, synes ikke å være mer byrdefullt eller risikabelt for borgerne, enn den håndtering som daglig

18 NOU 2004:6 Mellom effektivitet og personvern ss. 212–214.
19 Datalagringsdirektivets fortale pkt. 7–10, jf. art. 1.1.
20 Datasikkerhetsforpliktelsen er understreket i direktivet art. 7.

betros andre tjenesteytere; for eksempel finansinstitusjoner som forvalter våre bankkonti, oppgjørsagenter som formidler elektronisk betaling ved kjøp over internett, næringsdrivende som lagrer kunderegistre og regnskapsbilag, eller fastlegen som har en pasientjournal. Også her er det tale om lovpålagt lagring av personopplysninger. Håndtering av personopplysninger, herunder overholdelse av rutiner innrettet på å hindre lekkasje av data, er en del av hverdagen til hver moderne bedrift.

Debatten om datalagring er imidlertid en nyttig påminnelse om behovet for en gjennomgående profesjonalisering av håndteringen av persondata. Dette er det et politisk ansvar å besørge.

4 EMK og overvåking

Gjennomgangen har vist at overvåking er en kompleks materie. Det gir derfor neppe mening å spørre om man velger å leve i et overvåkingssamfunn, eller med en risiko for å bli drept av terrorister. De enkelte overvåkingstiltak må konkretiseres for å kunne ta stilling til om de kan godtas.

Hva man tror om terrorfaren og hvilke holdninger man har til sikkerhetspolitiske spørsmål mer generelt, spiller også inn. Jeg skal ikke gi meg inn på «terrorsiden» i denne balansetesten, men konsentrere meg om noen spørsmål som med litt forskjellige vinklinger, tar opp om vi har tilstrekkelig kontroll med overvåkingen.

Jeg avgrenser mot spørsmål om bruk av overskuddsinformasjon og om bevisavskjæring.

4.1 Rettslig styringslogikk

En viktig rettslig referanseramme for å kontrollere overvåking, er EMK art. 8. Etter bestemmelsen skal det først vurderes om kontrolltiltaket representerer et *inngrep* i personvernet, jf. EMK art. 8.1, og i så fall, om inngrepet kan *rettferdiggjøres*, jf. EMK art. 8.2. Det krever at inngrepet har et legitimt formål, tilfredsstiller en proporsjonalitetsvurdering og formelle rettssikkerhetskrav.[21]

Gjennom det materielle rettighetsvernet og rettssikkerhetskravene, skal EMK art. 8 være en garanti for personvernet. Mer generelt har personvernet

21 EMK art. 8 lyder: «1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse. 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlig trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

sterk forankring i oppfatningen om at det frie enkeltindividet har rett til å være i fred for myndighetene, så lenge det ikke opptrer til skade for andre. Dette er en grunntanke i vårt styresett.

Med dette utgangspunktet kan vi identifisere en *rettslig styringslogikk* som går omtrent som følger: Fordi vi er enige om de generelle verdiene som ligger til grunn for EMK, og fordi vi lojalt tester overvåkingstiltak mot EMK art. 8, og følger praksisen fra EMD, tror vi at bruken av overvåking holdes under kontroll.

Det er imidlertid farlig å slå seg til ro med en tro på at politikken blir tilfredsstillende, bare EMK respekteres. *Tredje tese er således at den rettslige styringslogikken er utilstrekkelig for å demme opp mot overvåking.*

Jeg har særlig festet meg ved tre forhold som begrunner tesen:

(i) *Minstestandardargumentet:* Utgangspunktet er at EMK oppstiller *minstekrav*; de politiske målsettingene bør imidlertid ligge langt over terskelen for hva som er akseptabelt menneskerettslig sett.

(ii) *Det kumulative argumentet:* EMDs praksis i *enkeltsaker* synes å være uegnet som målestokk for å bedømme om vi har et tilstrekkelig vern mot overvåking samlet sett. Punkt *5* inneholder en sluttkommentar med de to nevnte argumentene.

(iii) *Kasuistikk:* EMDs praksis synes å komme til kort på noen viktige punkter som gjelder utviklingen av overvåking. Det ene gjelder *åpen fjernsynsovervåking;* et meget praktisk spørsmål gitt den økende popularitet en som denne overvåkingsformen har (se punkt 4.3). Det andre gjelder kontrollen med politiets nettbaserte tvangsmiddelbruk. Rettssikkerhetskriteriene slik de pr idag er utformet av EMD, bør suppleres med et krav om *teknologikontroll*. Hederlige polititjenestemenn og domstolskontroll er vel og bra, men utilstrekkelig dersom man likevel ikke har kontroll med teknologien som benyttes i etterforskingen (se punkt 4.5).

4.2 EMK art. 8: Noen utgangspunkter

Det tas utgangspunkt i overvåkingsbegrepet beskrevet i punkt 2.5. Spørsmålet om kontrollmetoden innebærer noe inngrep, vil utløse vurderinger etter alternativene «privatliv» og «korrespondanse», jf. EMK art. 8.1. Begrepene flyter noe over i hverandre, men i utgangspunktet omfatter det sistnevnte alternativet enhver form for kommunikasjon ved brev og tekniske midler. Både privat og arbeidsrelatert kommunikasjon er vernet. Alternativet er følgelig relevant

ved metodebruk som *brev- og kommunikasjonskontroll*, uavhengig av hvilken kommunikasjonsteknologi som er benyttet.[22]

Alternativet «privatliv» har en bred betydning som omfatter individets navn, identitet, seksuelle legning m.v. Dessuten omfattes individets personlige utvikling, muligheten for å inngå bekjentskaper og å ha kontakt med omverdenen. Også aktiviteter knyttet til yrkes- og profesjonsforhold omfattes. Sentralt i vurderingen, uten at det i seg selv er avgjørende, er hvorvidt det foreligger en *rimelig forventning om noe privatliv*.[23] En slik forventning er det jo grunn til å ha når man er hjemme, hos venner, på et hotellrom o.l., men ikke i byrommet. Imidlertid kan forventningen om et privatliv, også gjelde på offentlige steder, som på venterommet på en politistasjon eller i en varetektscelle. *Romavlytting* og *videoovervåking* er eksempler på metoder som vurderes etter privatlivsalternativet.

I vurderingen av om det foreligger noe inngrep, går det et hovedskille mellom åpen og skjult metodebruk. Hemmelig overvåking er karakterisert som en trussel (*«menace»)*,[24] med iboende misbruksmuligheter som kan true og til og med ødelegge demokratiet.[25]

EMD skiller mellom observasjonen som sådan og de øvrige fasene i informasjonshåndteringen. Det klare utgangspunkt er at lagring av personopplysninger i politiets registre, er å anse som inngrep.[26] Men observasjoner ved bruk av åpne overvåkingsmetoder, er ikke uten videre inngrep, noe *Peck* illustrerer (se nedenfor). Derimot vil systematisk eller varig lagring eller bruk, av opplysningene være det. Hvert trinn i informasjonshåndteringen blir vurdert i lys av inngrepskriteriet, se *Peck* (bruk av opptak fra åpen fjernsynsovervåking); *Amann* om opprettelse av et arkivkort med notater fra telefonavlytting; *Weber* om håndtering av opplysninger fra hemmelig strategisk overvåking.[27]

4.3 Åpen fjernsynsovervåking: Problemet med Peck og Perry

Forsåvidt gjelder fjernsynsovervåking på offentlig sted, har EMD inntatt det standpunkt at så lenge det skjer for et legitimt påregnelig formål (som kriminalitetsbekjempelse), representerer det ikke noe inngrep i privatlivet og faller utenfor området for EMK art. 8.1. Flere avgjørelser leder opp til denne

22 At telefoni omfattes av «korrespondanse» ble avgjort i Klass (41), og er fulgt opp i senere avgjørelser.
23 P.G. and J.H. (56–57).
24 Klass (37) og (41).
25 Se bl.a. Klass (49–50); Weber (106); Volokhy (52).
26 Leander (48); Amann (70); Rotaru (43–44).
27 Peck (60–63); Amann (68 flg.); Weber (79).

rettstilstanden, som knytter an til den *fjerde tesen; nemlig at EMDs praksis er utilstrekkelig for å kontrollere offentlig fjernsynsovervåking.*

I *P.G. and J.H* drøftet EMD hva som er en *rimelig forventning til privatliv* i det offentlige rom. I den forbindelse ble de observasjoner en vaktmann kan gjøre ved fjernsynsovervåking, eksplisitt sidestilt med de observasjoner personer som fysisk er tilstede, kan gjøre. Med andre ord; en person som spaserer ned gaten har ikke en berettiget forventning om noe privatliv (på gaten), verken overfor personer som er tilstede, eller overfor vaktmenn som følger med på gatebildet via fjernsynsovervåking (i dommen kalt «*monitoring*»). Etter EMDs syn utløses hensynet til privatlivet først dersom fjernsynsovervåkingen resulterer i systematiske eller varige opptak.[28]

I *Peck* tok EMD utgangspunkt i denne rettsoppfatningen, for så å uttale seg om nytten av offentlig fjernsynsovervåking, dvs. om det er et egnet virkemiddel for å bekjempe kriminalitet. Forholdet var at Peck var blitt filmet mens han var i ferd med å begå selvmord. Dette ble avverget som følge av overvåkingen. Lokale myndigheter ga imidlertid filmopptaket til media, som brukte det i avisoppslag og på fjernsyn uten samtykke og tilstrekkelig anonymisering av Peck. Formålet var å drive informasjonsvirksomhet for å vinne tilslutning til bruk av fjernsynsovervåking som kriminalitetsforebyggende tiltak. Problemet, sett fra Pecks side, var at han på grunn av konteksten ble fremstilt som en forbryter, til tross for at han ikke hadde begått noen kriminell handling. Han mente at slik bruk av opptaket uten hans samtykke, var et inngrep i privatlivet. Han trakk imidlertid ikke den kriminalitetsforebyggende effekten i tvil, og prosederte ikke på at filmingen som sådan var et inngrep.

EMD sa følgelig at «the Court appreciates the strong interest of the State in detecting and preventing crime. It is not disputed that the CCTV system [closed-circuit television system] plays an important role in these respects and that the role is rendered more effective and successful through advertising the CCTV system and its benefits» (79).

I *Perry* ble resonnementet ført til ende. Her sier EMD rett ut at normal bruk av fjernsynsovervåking som sådan, enten det skjer på offentlig gate eller på områder som kjøpesentra eller en politistasjon, hvor det tjener et legitimt påregnelig formål, *ikke* reiser spørsmål under EMK art 8.1. Åpen fjernsynsovervåking av byrommet m.v., er altså ikke et menneskerettslig tema.

Det er påfallende at denne rettssetningen er etablert *uten at det er ført bevis for at fjernsynsovervåking er et egnet kriminalitetsforebyggende tiltak*. I *Peck* ble EMD fratatt muligheten for å vurdere det, siden Peck ikke innga noen

28 P.G. and J.H. (57).

klage på dette punkt; han var bare lettet over at tiltaket hadde bidratt til å redde hans liv (*Peck* (54)). Og i *Perry* baserte EMD seg på *Peck*.

Den norske samfunnsviteren Heidi Lomell, har i en interessant artikkel om *Peck* påpekt at på det tidspunkt saken gjaldt, forelå det *en sterk tro*, men *lite vitenskapelig belegg*, for at slik fjernsynsovervåking hadde kriminalitetsforebyggende effekt. Politikerne og handelsstanden var opptatt av å spre informasjon om tiltaket, for å demonstrere politisk handlekraft overfor den bekymringsfulle kriminalitetsutviklingen, og markedsføre handelsstandens interesser (jf. slagordet *«CCTV doesn't just make sense – it makes business sense»)*. Men *«hadde EMD krevd at den britiske regjering skulle underbygge sin påstand om at videoovervåking har kriminalitetsreduserende effekter, ville de fått problemer med å finne empirisk belegg for dette»*, skriver Lomell. Hun gir en rekke henvisninger til nyere forskning.[29]

Dette gir grunnlag for å reise flere spørsmål knyttet til åpen fjernsynsovervåking:

For det første er den menneskerettslige aksepten for et *generelt overvåkingstiltak*, etablert, uten at effekten er dokumentert. Når vi idag diskuterer bruk av fjernsynsovervåking på offentlige steder, *bør vi med andre ord snarere se hen til hva forskningen kan fortelle oss, enn EMDs praksis*.

EMDs praksis *kan* utfordres av en ny sak med nytt vitenskapelig basert faktum, men erfaringen fra Storbritannia viser at det finnes en risiko for å bli møtt med argumenter basert på en *formålsforskyvning*, dvs. at myndighetenes og handelsstandens investering i tiltak, både økonomisk og med tanke på troverdighet og goodwill, i seg selv kan lede til et ønske om å beholde fjernsynskameraene. Derfor går man på jakt etter nye gode formål som kan begrunne bruken.[30]

For det andre kan man stusse over rettssetningen fra *Perry,* om at åpen fjernsynsovervåking *faller helt utenfor området for EMK art. 8*. Betyr det at myndighetene fritt kan bruke store ressurser på slik overvåking, uten at det kan anses å ha en menneskerettslig side? Muligens innebærer vilkåret om et *legitimt påregnelig formål*, en begrensning for hvor stort omfanget av overvåkingen tross alt kan bli, uten at det representerer et inngrep. Vilkåret ble tilføyd i *Perry*, til tross for at overvåkingen i utgangspunktet ble ansett for å falle utenfor art. 8, så noen begrensninger later det til at vi kan regne med gjelder.

Mer vesentlig er kanskje *fortolkningen av «privatliv»*. Her kan flere forhold tas opp til kritisk vurdering.

Et spørsmål er om man uten videre bør godta likestillingen av en vaktmanns observasjoner via kamera, med observasjoner gjort av personer som

29 Lomell (2005) ss. 40–41. Se i samme retning Gill (2005).
30 Lomell (2005) s. 40.

selv er fysisk tilstede. Det kan hevdes at man er i det offentlige rom overfor personer som selv gir seg tilkjenne, mens man har rett til å holde på sin privatsfære overfor anonyme observatører. Bør ikke selve *disiplineringseffekten* av å vite seg observert, uten at man vet av hvem, anses som et inngrep i privatlivet? Kanskje holder ikke resonnementet dersom fjernsynsovervåkingen er begrenset, og bare få kjente aktører står bak, f.eks. kun politiet. Men når fjernsynsovervåking tas i utstrakt bruk, har varsling ved bruk av skilting liten betydning; i praksis kan ikke borgeren holde oversikt over observatørene, og innrette seg.

Politimetodeutvalget kan synes å ha pekt på noe vesentlig, da det i 2004 sa at dersom slik fjernsynsovervåking blir vanlig, vil det være *«et solid bidrag til at overvåkingssamfunnet erstatter det rettssamfunn vi idag kjenner»*.[31] Spørsmålet er, hvor bærer utviklingen hen nå?

Ytterligere synes det å være tvilsomt om man, slik EMD gjør, bør operere med en avgjørende grense mellom *observasjoner* og *lagring/bruk* av opplysninger. Ihvertfall så lenge det er tale om observasjon ved menneskelig sansebruk, må vi regne med at opplysningene lagres i hukommelsen. Det er jo nettopp grunnlaget for rettssystemets utstrakte bruk av vitnebevis, og tilsier at også rent observerende metoder foretatt av offentlig myndighet, bør anses som inngrep som må rettferdiggjøres etter EMK art. 8.2.

Felles for innvendingene er at de øker i tyngde, jo mer omfattende fjernsynsovervåkingen er og jo flere aktører som står bak. Argumentasjonen her henger altså sammen med bekymringen for det totale overvåkingstrykket, som vi kommer tilbake til i punkt 5.

4.4 Om rettssikkerhet

Rent logisk er det mulig å forestille seg en rettsstat som også er et overvåkingssamfunn. Her får man si som Raz, at *«the rule of law»* ikke er ensbetydende med *«rule of the good law»*.[32] Raz' poeng er at formelle krav til rettssikkerhet kan bidra til et godt styresett, blant annet fordi det sørger for likhet for loven og kontroll mot vilkårlighet og maktmisbruk. Rettssikkerhetskrav alene er imidlertid ikke tilstrekkelig for å sikre et godt samfunn; det kommer an på det materielle innholdet i lovene og styresettet forøvrig (demokrati).

En lov som for eksempel sier at opplysninger om de daglige bevegelsene til borgerne skal registreres og oppbevares i 30 år før de slettes, bryter altså ikke med noe formelt rettssikkerhetskrav. Om loven åpner for at opplysningene

31 NOU 2004: 6 Mellom effektivitet og personvern s. 212.
32 Raz (1977) s. 77.

kan benyttes av politiet, er vi også innenfor alminnelige rettssikkerhetsnormer, såfremt vilkårene er klare og bruken kontrolleres av en domstol. Men på grunn av registreringens store omfang vil vi likevel formentlig konkludere med at en slik lov ville medføre et overvåkingssamfunn.

Lovskravet i EMK art. 8.2, skal ivareta rettssikkerheten, og dette gjøres ved at det stilles krav til hjemmel for inngrep (*basis in law*), krav til lovens presisjon og klarhet (*quality of the law* og *foreseeability*), lovens tilgjengelighet (*accessibility*), og kontroll med at loven overholdes (først og fremst *domstolskontroll*). Men, som vi forstår, er dette formelle vilkår som ikke i seg selv etablerer et rettighetsvern.

EMDs praksis gir statene *en vid skjønnsmargin* mht. tiltak for å ivareta samfunnssikkerheten. Blant annet aksepteres «overvåkingslovgivning», dvs. lovgivning som åpner for hemmelig overvåking av borgerne av hensyn til nasjonal sikkerhet, eller forebygging av alvorlig kriminalitet. Det stilles imidlertid strenge krav til lovens klarhet og til kontrollen med at loven blir fulgt.

Den ledende saken er *Klass* (1978), hvor tysk terrorlovgivning som ga sikkerhetstjenesten adgang til hemmelig overvåking av borgerne, ble godtatt til tross for at ikke engang de som reiste saken, visste om de hadde vært overvåket og hadde konkret foranledning til å angripe loven. EMD har anlagt det syn at selve *eksistensen* av lovgivning som åpner for hemmelig overvåking, innebærer et inngrep overfor borgerne. I prinsippet kan derfor enhver borger anlegge sak for å prøve konvensjonsmessigheten av slike lover.[33]

I *Weber* (2006) var den tyske lovgivningen oppe til ny prøving, på bakgrunn av at den hadde blitt endret og nå også ga adgang til *strategisk overvåking,* og for flere formål enn tidligere. Etter en omfattende vurdering avviste EMD klagen som *«manifestly ill-founded»,* dvs. at lovgivningen ble godtatt.[34]

Weber innebærer at EMD har gått et steg videre. I *Klass* var det tale om overvåking basert på faktiske opplysninger som ga grunnlag for å rette kontrollen mot bestemte individer (individuell overvåking).[35] I *Weber* godtas også overvåking basert på generelle kriterier som brukes til å «single ut» enkeltpersoner som ikke på forhånd er i søkelyset. Det er adgang til fra tyske lyttepunkter å avlytte internasjonale telefonsamtaler med forbindelse til Tyskland, og styre innsatsen mot samtaler som inneholder visse hemmelige nøkkelord. Det er således hjemmel for overvåking uten konkret mistanke, for å identifisere individer som det senere kan rettes en innsats mot.[36]

33 Klass (41); Malone (64) (her avgrenses personkretsen); Weber (78); AEIHR (69).
34 Weber (156).
35 Klass (17) og (51) («factual indications for suspecting a person»).
36 Weber (18) (88) (97).

Motstykket til den vide skjønnsmarginen er de strenge rettssikkerhetskravene, og her kan det vises til en nyere dom, *AEIHR* (2007), som illustrerer et overvåkingsregime med eklatante brudd på rettssikkerheten. Saken gjaldt overvåkingslovgivning i Bulgaria, som – bortsett fra kravet til lovforankring – sviktet på nærmest alle punkter. Helt sentralt i kritikken var mangelen på uavhengig kontroll med systemet, som i praksis ble styrt av innenriksministeriet.[37] Til slutt vurderte EMD om mangelen på formell rettssikkerhet hadde hatt noen virkning på overvåkingssystemet slik det faktisk ble praktisert. Det ble påpekt at selve mengden av overvåkingstillatelser fremsto som svært stor; man talte om en snitt på ca 20 overvåkingstillatelser pr arbeidsdag, og da var ikke avlyttingstillatelser for mobiltelefoni inkludert. EMD noterte seg at *«numerous abuses had taken place»*, og konkluderte med at *«the system of secret surveillance in Bulgaria is, to say the least, overused, which may in part be due to the inadequate safeguards which the law provides»*.[38]

At et nylig diktatur har slike problemer er neppe egnet til å overraske, men det skal ikke forlede noen til å tro at alt er bra i de gamle demokratier i Norden. Dette illustreres med noen eksempler fra Danmark og Norge, som gjelder *tesen om at dansk og norsk overvåkingslovgivning synes å ha mangler med hensyn til grunnleggende krav til hjemmel og kontroll.*

I Danmark er det rettet skarp kritikk mot terrorlovgivningen, blant annet fordi Politiets etterretningstjeneste (PET) er gitt vid overvåkingsadgang uten klart lovgrunnlag eller domstolskontroll.[39]

PETs virksomhet er ikke særskilt regulert, og tjenesten er således undergitt de alminnelige regler for politiets virksomhet. PET skal først og fremst drive *forebyggende* virksomhet, og opplyser selv å ha straffeprosessuelle tvangsmidler til rådighet, og å følge prosedyrene i retsplejeloven.[40]

Ifølge retsplejeloven er imidlertid bruk av tvangsmidler betinget av at det er tale om *etterforsking*, noe som forutsetter at det er «rimelig formodning» om at et straffbart forhold er begått, dvs. at grensen for straffbart forsøk er passert.[41] Forebygging i ren forstand, er ikke det samme som etterforsking, fordi det kan settes inn tidligere og har et annet formål, for eksempel utvisning av uønskede personer. PETs kjerneoppgave står derfor i et tydelig spenningsforhold til det straffeprosessuelle hjemmelsgrunnlaget for tvangsmiddelbruk. Dette kan være problematisk i forhold til EMKs klarhetskrav til nasjonalt regelverk.

37 AEIHR (85) og (87).
38 AEIHR (92).
39 Hoff-Lund (2006).
40 PETs hjemmeside: http://www.pet.dk/ (besøkt 13. februar 2008).
41 Det gjelder for eksempel regler om inngrep i meddelelseshemmeligheden m.v. i rpl. kap. 71, jf. §§ 742 stk. 2, jf. 743.

EMD legger stor vekt på *kontrollen* med overvåkingsaktiviteten, både før, under og etter, inngrepet. Behovet for at kontrollen er uavhengig og reell fremheves. Dansk lovgivning er kritisert også på dette punkt, idet PET påstås å kunne foreta omfattende innhenting av personopplysninger fra andre offentlig organer, uten domstolskontroll. Dermed mangler den disiplinerende effekten som domstolskontroll innebærer. I tillegg åpner ordningen for strategisk informasjonsanalyse, uten lovgrunnlag (se punkt 5). Begge deler kan være vanskelig å forsvare i lys av EMDs praksis.

Hvis vi retter blikket mot Norge, er overholdelse av den grunnleggende *underretningsplikten* om inngrep, problematisk. EMD framhever at underretning er et helt nødvendig tiltak for å hindre myndighetsmisbruk. EMD godtar at underretning i forkant forspiller formålet med overvåkingen, og oppstiller ikke noen ubetinget plikt til å underrette umiddelbart etter at inngrepet er avsluttet. EMD aksepterer også at behov for vern om politiets metodebruk og interesseområder, kan begrunne at det går svært lang tid før underretning gis (*«years, even decades»)*.[42] Men, på et eller annet tidspunkt må underretning gis. Det er et ubetinget vilkår for å sikre mot misbruk og kunne sørge for oppreisning / kompensasjon for overlast (*«remedy»*).

I Norge er det gitt adgang til *helt hemmelig metodebruk* blant annet for å forebygge terror og anslag mot rikets sikkerhet.[43] Selv om loven sørger for en ordning med hemmelig forsvarer, synes fraværet av underretningsplikt å stå i et tvilsomt forhold til EMDs minimumskrav.

4.5 Rettssikkerheten krever økt teknologikontroll

En utfordring som gjør seg gjeldende med stadig større styrke, gjelder bruken av hemmelige teknisk betonte etterforskingsmetoder. EMD har uttalt at det er «essential to have clear detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated».[44]

Mer spesifikt gjelder problemstillingen notoritetproblemer ved hemmelig metodebruk over elektroniske nettverk, slik som *dataavlesing*. Slik metodebruk reiser nemlig spørsmål om dagens rettssikkerhetstenkning er for snever til å gi effektiv kontroll. *Sjette tese er således at rettssikkerheten krever økt teknologikontroll.*

Opprinnelig var forskningsbehov foranledningen til at internett ble utviklet med tjenester som ga mulighet for ressursdeling ved å koble opp til andre

42 Klass (58); Weber (135); AEIHR (90).
43 Jf. politiloven § 17e, jf. § 17d.
44 Amann (56); Weber (93); AEIHR (75).

maskiner. Ressursdelingen var basert på samtykke til å logge seg inn på en annens maskin over nettet. *Hackerne* tok muligheten i bruk på rettsstridig vis. Ved bruk av en ordinær oppkoblingstjeneste kontaktet de en annen maskin i nettet, og skaffet seg rettsstridig adgang ved misbruk av passord eller av sårbarheter på datasystemet («bakdører»). Tredje omdreining i utviklingen er at politiet ønsker mulighet for å koble seg opp til siktedes datamaskin, kopiere innholdet og registrere tastetrykk. Formålet er særlig å skaffe seg kjennskap til passord og kodenøkler før innholdet eventuelt blir kryptert. Det er ingen nytte i å ta databeslag eller foreta avlytting, dersom innholdet er kryptert og kodenøkkelen mangler.

Metoden som kalles *dataavlesing*, er tillatt i Danmark, jf. rpl. § 791 b, og er under vurdering i Norge og Sverige.[45]

Dataavlesing byr på spesielle misbruksproblemer. Dataprogrammet som installeres på siktedes datamaskin, gir nemlig politiet kontroll over datamaskinen, og kan f.eks. iverksette romavlytting ved å aktivisere mikrofonen (alle moderne PCer har innebygd mikrofon), starte et webkamera, og endre, slette eller tilføye data. Kontroll med varigheten av tillatelsen er også en utfordring; hvordan oppnås verifikasjon av at programmet virkelig er slettet på siktedes datamaskin når perioden er utløpt? Og hvilke garantier finnes for at logger som skal ivareta notoritet, har riktig innhold? Til slutt foreligger muligheten for at programmet kan oppdages av *tredjeparter,* ved skanning av maskiner som er tilkoblet internett. Slike tredjeparter kan f.eks. være fremmede etterretningstjenester eller kriminelle miljøer som kjenner politiets programvare. I så fall kan de lage dataprogrammer (skannere/«ormer») som leter på nettet etter datamaskiner som er infisert med politiets dataavlesingsprogrammer.[46]

Når man først forstår hvilke muligheter (i det godes tjeneste) som ligger i ny teknologi, oppstår et press for å ta mulighetene i bruk. Men, den andre siden av medaljen er at forsvarlig bruk krever solid kompetanse om misbruksmulighetene. Politiet har ansvar for å unngå misbruk, men det kan ikke tas for gitt at den nødvendige kompetansen bestandig er tilstede. Domstolen på sin side, har ikke mulighet for å kontrollere om den tekniske siden av metodebruken er forsvarlig. Ansvaret må derfor anses å ligge hos lovgiver som bør vedta *notoritetskrav* for å sikre teknologikontroll.

45 Norge: NOU 2004:6 Mellom effektivitet og personvern s. 207; Ot.prp. nr. 60 (2004–2005) s. 141. Sverige: Ds 2005:6 Brott och brottsutredning i IT-miljö s. 299; SOU 2005:38 Tillgång til elektronisk kommunikation i brottsutredningar m.m. kap. 9.

46 Sunde (2006) ss. 292–293.

I Danmark sier forarbeidene til bestemmelsen om dataavlesing, at det er tale om *«et såkaldt «sniffer-program»»*,[47] Beskrivelsen virker noe tynn som beslutningsgrunnlag for lovgiver, og synes å gi svake begrensninger for politiet. Lovgivers avventende holdning til å ta metoden i bruk i Norge og Sverige, kan derfor være velbegrunnet.[48]

Hvilke krav bør stilles? Jeg mener det handler om at dataprogrammene som politiet benytter overfor siktedes datamaskin, må være *veldokumenterte, godkjente og velprøvde, og at loggen som genereres ved bruken er fullstendig og korrekt.*

Kravet til at programmet er *veldokumentert* innebærer at programmets kildekode bør være under nasjonal kontroll, slik at politiet kan gjøre seg kjent med og ta ansvar for alle dets egenskaper. Bruk av program med lukket kode, f.eks. innkjøpt fra en etterretningstjeneste i utlandet, eller lastet ned fra hackersider på nettet, bør ikke være akseptabelt. I det første tilfellet er man prisgitt den informasjon om programmet som selgeren (den «samarbeidende» tjenesten) velger å gi; i det andre er det egentlig helt tilfeldig hva man vet.

Før programmet brukes i etterforsking bør det foreligge *erfaring* ved bruk i et kontrollert miljø, og programmet bør være *godkjent* av kompetent instans.

Troverdigheten til loggen utgjør et eget problem. Det må kreves at loggen registrerer alt, også det som eventuelt ligger utenfor tillatelsen, så får håndteringen av overskuddsinformasjon, og av eventuelle «overskuddsaktiviteter», bli en sak for seg. Da er det ihvertfall tale om et konkret og håndterlig problem, og ikke om uvisse forhold som gir grobunn for mistanke om myndighetsmisbruk. Innholdet i loggen må være korrekt, og ikke kunne manipuleres.

Hensyn til notoritet er grunnleggende for tilliten til politiets arbeid og det bør, etter min mening, være et minimumskrav at slike regler foreligger før metoden tillates.

5 Det generelle overvåkingstrykket

Overvåking som vendes mot borgerne uten legitim grunn er farlig. Da er det ikke et tiltak som skaper sikkerhet, men det motsatte. Som hyppig påpekt av EMD kan overvåking underminere demokratiet.[49]

Det er tankevekkende og noen vil si foruroligende, at samtlige nordiske land har svært lav uttelling på kriteriet *politisk lederskap* i personvern- og

47 Jf. bemerkningene til lovforslag L 35, folketingssamlingen 2001/2002, § 2 nr. 4 om endringer til rpl. § 791 b.

48 I skrivende stund er det ikke gitt hjemmel for dataavlesing i Norge og Sverige.

49 Se punkt 4.2 og note 25.

overvåkingsspørsmål.[50] Det kan indikere et behov for å bevisstgjøre og prioritere politikken på området.

Med utgangspunkt i situasjonen i Norge, er imidlertid ikke bildet helt svart. Etter tillitskrisen på 1990-tallet er innsyn i gamle arkivmapper gitt, sikkerhetstjenesten er blitt reorganisert og oppgavene redefinert. Regjeringen har også nedsatt en Personvernkommisjon for å belyse utfordringer for personvernet, og et Metodekontrollutvalg som skal evaluere politiets metoder. Regjeringen har uttalt at det ikke kommer på tale å innføre nye metoder før evalueringen er gjennomført.[51] Man får anta at den norske regjering ikke er alene i Norden om å vise politisk vilje til å ivareta hensyn til personvern og rettssikkerhet.

Men det er liten grunn til å forvente en politisk kursendring. For eksempel ser regjeringen ut til å ville ri to hester samtidig i spørsmålet om dataavlesing. Regjeringen har nemlig gitt Metodekontrollutvalget i oppdrag *også å foreslå regler om dataavlesing*.[52] Når oppdraget gis til det utvalg som nettopp skal *evaluere* dagens metoder, formodentlig med en teoretisk mulighet for å anbefale avvikling av noen av dem, synes i realiteten viljen til restriksjon overfor nye inngripende metoder, å være liten.

Myndighetene har også en tendens til, som en del av begrunnelsen for nye tiltak mot terror m.v., å vise til den positive forpliktelsen til å sikre retten til liv, jf. EMK art. 2.[53] Men denne henvisningen kan i høyden tjene som en påminnelse om at myndighetene plikter å arbeide for et sikkert samfunn, dvs. et av de formål som nettopp kan begrunne inngrep i personvernet, jf. EMK art. 8.2. Den positive forpliktelsen vedr. retten til liv, er neppe et selvstendig, rettslig bærekraftig argument i denne sammenheng. Når myndighetene likevel bruker det som rettslig argument, oppstår en risiko for å tilsløre at innføringen av nye metoder skyldes *politiske* valg. Da blir spørsmål om lederskap viktig.

Rettsvitenskapen kan støtte politikken ved å belyse rettspolitiske dilemmaer, men synes i liten grad å være egnet som verktøy for å begrense overvåking. Årsaken er blant annet at juristenes fokus raskt dreies mot det å teste regelverk og praksis mot rettsordenens *minimumskrav*. Når spørsmålet om et inngrep er rettslig holdbart, vurderes i lys av EMK, blir målestokken en praksis utledet av saker som enten er en anomali i et ellers godt rettssystem, eller som er en indikasjon på et rettssystem i krise. Og som EMD selv presiserer; det er tale om

50 På en skala fra 1 til 5 (beste verdi) har Sverige 1 poeng, mens Danmark, Finland, Island og Norge har 2. Se Privacy International (2007).

51 Ot.prp. nr. 8 (2007–2008) s. 14.

52 Mandatet punkt 1.3.

53 Se eksempelvis Ot.prp. nr. 60 (2004–2005) pkt. 3.3, og Ot.prp. nr. 8 (2007–2008) pkt. 8.4.1.

å opprettholde en *minstestandard («minimum safeguards»)*.[54] Politikerne (lovgiver) bør jo ha ambisjon om å ligge godt over en minstestandard. Spørsmålet er om rettsvitenskapen kan bidra til det.

Her skal jeg kaste inn et siste problem til diskusjon:

Jeg tror nemlig ikke at utfordringen først og fremst gjelder metodebruken i enkeltsaker (vi lever jo i en rettsstat), men om den *kumulative effekten* av overvåking *(syvende tese)*. Det som gir grunn til bekymring er både summen av alle tiltakene, dvs. hvordan vi som borgere opplever det, og særlig bruken av *generelle tiltak uten mistankegrunnlag*, slik som åpen fjernsynsovervåking. Åpen fjernsynsovervåking har imidlertid det fortrinn at det nettopp foregår åpent, så det er tross alt noe vi vet om.

Hva da med såkalt strategisk informasjonsanalyse («data mining»), som foregår skjult?

Det er vanlig at sikkerhetstjenesten er satt opp med en såkalt «analyseenhet», og spørsmålet knytter seg til *datatilfanget* for slik virksomhet. Er utvalget av data koblet til konkret mistanke, eller søkes det gjennom store mengder persondata på jakt etter anomalier som kan indikere terror? Siden forekomsten av terror tross alt er svært liten, er sjansen stor for at «anomalien» viser seg å være en uventet, men uskyldig og lovlig handling, som for eksempel et «overraskelsesselskap», et fiendtlig oppkjøp på børsen, eller at man ombestemte seg og kom hjem i stedet for å reise på et seminar i utlandet. Omkostningene ved feiltreff er imidlertid store, både økonomisk (den bortkastede ressursbruken), og for personvernet, ved at man kommer i politiets søkelys utelukkende på grunn av at aktiviteten er uventet.

Metoden skal være et populært antiterrortiltak i USA (122 føderale prosjekter er identifisert), men det hersker svært delte oppfatninger om dens legitimitet for dette formål.[55]

Dersom det ikke gjelder noen begrensning for hvilket datatilfang som kan anvendes for strategisk informasjonsanalyse, vil slik overvåking være mye mer inngripende enn den tyske som er godtatt i *Weber*.[56] Hvordan vil det for eksempel stille seg med bruken av lagrede kommunikasjonsdata? Etter datalagringsdirektivet art. 1, kan dataene blant annet benyttes til *å avdekke* kriminalitet («*detection*»). Betyr det at direktivet åpner for lovgivning som tillater bruk av dataene for strategisk informasjonsanalyse uten mistankegrunnlag? Og er det nettopp slik man skal forstå den del av kritikken mot

54 Weber (95); AEIHR (76).
55 Her er to eksempler: I favør av metoden: Taipale (2007); motsatt: Schneier (2007).
56 Se punkt 4.4.

dansk antiterrorlovgivning, som gjelder at PET ganske fritt og uten nevneverdig kontroll, kan innhente personopplysninger fra andre offentlige etater?[57]

I lys av den vide skjønnsmarginen foreligger det her virkelig et spørsmål hvor politikerne har anledning til å utvise lederskap – i den ene eller andre retning.

6 Teser:

Tese 1: Fordi ingen vet hva overvåking er, vet ingen hva de er imot.
Tese 2: Overvåkingsspørsmål forveksles ofte med andre spørsmål.
Tese 3: Rettslig styringslogikk er utilstrekkelig for å demme opp mot overvåking, det krever en politisk vilje som strekker seg utover EMKs minimumskrav.
Tese 4: EMDs praksis er utilstrekkelig for å kontrollere åpen fjernsynsovervåking.
Tese 5: Norsk og dansk overvåkingslovgivning har mangler mht. grunnleggende krav til hjemmel og kontroll.
Tese 6: Rettssikkerheten krever økt kontroll med politiets teknologi.
Tese 7: Jussen synes å komme til kort overfor problemet med å kontrollere det generelle omfanget av overvåking.

7 Litteraturliste:

Gill (2005) Gill, M., Spriggs, A., 'Assessing the Impact of CCTV', Home Office Research Study 292, UK, 2005.

Henricson (2007) Henricson, I., *Politiret*, 4. utg. København, 2007.

Hoff-Lund (2006) Hoff-Lund, O., 'Den vingeskudte retsstat', ss. 8 flg. i Medlemsblad for Amnesty International, Danmark, 3/2006 *(Terrorpakken)*.

Lomell (2005) Lomell, H. M., 'Videoovervåking og menneskerettigheter', ss. 32 flg. i NTfM 1/2005.

Lyon (2005) Lyon, D., *Surveillance Society: Monitoring Everyday Life,* 2005 (opptrykk fra 2001).

Privacy International(2007) Privacy International 'The 2007 International Privacy Ranking' (28.12.07). http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (besøkt 15.01.08).

57 Hoff-Lund (2006) ss. 11–12.

Raz (1977) Raz, J., 'The Rule of Law and its Virtue', ss. 77 flg., i Bellamy, R. (Ed.), *The Rule of Law and the Separation of Powers,* 2005.

Schneier (2007) Schneier, B., 'How to Not Catch Criminals», i Forbes, 26. mars 2007. http://www.schneier.com/essay-163.html (besøkt 19. desember 2007).

Slettemark (2006) Slettemark, G., 'Hele folket under mistanke', Aftenposten 23. november 2006 (kronikk).

Sunde (2006) Sunde, I.M., *Lov og Rett i Cyberspace*, 2006.

Taipale (2007) Taipale, K. A., 'Why Can't We all Get Along? How Technology, Security, and Privacy Can Coexist in the Digital Age', ss. 151 flg., i Balkin, J.M., et.al. (Eds.) *Cybercrime – Digital Cops in a Networked Environment,* USA, 2007.

Wood/Ball (2006) Wood, D.M., Ball, K., (Eds.) 'A Report on the Surveillance Society', for the Information Commissioner by the Surveillance Studies Network, 2006.

8 Avgjørelser fra EMD:

AEIHR	Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, dom 28. juni 2007.
Amann	Amann v. Switzerland, dom 16. februar 2000.
Klass	Klass and Others v. Germany, dom 6. september 1978.
Leander	Leander v. Sweden, dom 26. mars 1987.
Malone	Malone v. UK, dom 2. august 1984.
Peck	Peck v. UK, dom 28. januar 2003.
Perry	Perry v. UK, dom 17. juli 2003.
P.G. and J.H.	P.G. and J.H. v. UK, dom 25. september 2001.
Rotaru	Rotaru v. Romania, dom 4. mai 2000.
Volokhy	Volokhy v. Ukraine, dom 2. november 2006.
Weber	Weber and Saravia v. Germany, beslutning fra 2006 vedr. klage nr. 54934/00.

PERSONVERNØKENDE TEKNOLOGI OG IDENTITETSFORVALTNING*

Thomas Olsen

1 Innledning

Den teknologiske utviklingen åpner opp for stadig nye tjenester som vil kunne sette personvernet i fare. Er det gitt at ny teknologi og ny teknologianvendelse nødvendigvis må medføre redusert personvern? Eller kan det tenkes at teknologien kan designes på en måte som fremmer eller øker personvernet? *Personvernøkende teknologi* (engelsk: Privacy-Enhancing Technologies – «PETs») antyder at dette er mulig. Som vi skal se, har PETs i snever forstand handlet om tekniske og organisatoriske tiltak som tar sikte på å begrense andres mulighet til identifisere den enkelte. Tankegangen tar utgangspunkt i at personvernhensyn kun gjør seg gjeldende dersom transaksjoner eller opplysninger kan knyttes til den de gjelder. Dette tradisjonelle fokuset på PETs som løsninger for anonymitet og pseudonymitet er fremdeles viktig. Imidlertid skal vi se at utviklingen går i retning av å betrakte disse spørsmålene om identitet og identifiserbarhet under synsvinkelen *identitetsforvaltning*. Identitetsforvaltning tar utgangspunkt i individets ulike roller og hvordan identifisering og autentisering kan tilpasses disse rollene og relasjonene. I det følgende skal vi se nærmere på bakgrunnen for PETs og identitetsforvaltning, hvordan slike løsninger kan styrke personvernet, samt forholdet til det rettslige vernet om personopplysinger.

1.1 Bakgrunn

Begrepet PETs kan føres tilbake til 1995 da datatilsynsmyndighetene i Ontario (Canada) og Nederland la frem sin felles rapport «Privacy-enhancing technologies: the path to anonymity».[1] Rapporten ble presentert på den 17. internasjonale datatilsynsmyndighetskonferansen i København samme år. I følge John

---

* Artikkelen er skrevet på oppdrag for Personvernkommisjonen, og vil bli publisert som vedlegg til kommisjonens sluttrapport som ventes fremlagt desember 2008.

1 Registratiekamer, Privacy-enhancing technologies: the path to anonymity (Vols I & II), 1995

Borking, den gang tilknyttet Registratiekamer – senere «PETs-evangelist», skapte budskapet stor oppsikt. Rapporten viste at de fleste informasjonssystemer kan designes slik at brukerens identitet holdes helt eller delvis skjult. Nøkkelen til slik personvernøkende design var «the identity protector» – en koblingssentral hvor personidentifiserende identifikatorer (som f eks fødselsnummer) ble gjort om til pseudonymer som ikke direkte kunne knyttes til noen identifiserbar person. Slike koblingssentraler mellom identifiserbare identifikatorer og pseudonymer kunne plasseres i informasjonssystemets ulike deler eller være under brukerens kontroll. Videre viste rapporten hvordan slike koblinger kunne skje automatisk i systemet eller etter nærmere bestemte regler av en uavhengig og tiltrodd pseudonymforvalter.

Den prinsipielle betraktningen om at personvernet kan ivaretas ved å begrense muligheten til identifisering var imidlertid ikke ny. Allerede i 1981 publiserte David Chaum sin banebrytende artikkel om hvordan man kunne oppnå anonymitet for avsender og mottaker av elektronisk kommunikasjon.[2] Innenfor kryptografien hadde man lenge forsket på hvordan man ved kryptering av elektronisk kommunikasjon kunne sikre *innholdet* fra uautorisert innsyn. Chaums tilnærming var en helt annen: det fakum at noen kunne observere *hvem* som kommuniserte med *hvem* kunne være uheldig fra et sikkerhets- og personvernsynspunkt.

Også Norge kan skilte med pionerarbeid innenfor personvernøkende teknologi. Tidlig på 1990-tallet arbeidet et offentlig utvalg ledet av professor Erik Boe med hvordan man kunne forene samfunnets behov for forskning på helseopplysinger samtidig som den enkeltes personvern ble ivaretatt. Mens man tidligere hadde skilt mellom anonyme eller avidentifiserte opplysninger (som ga relativt begrensede muligheter for forskning) og fullt ut identifiserbare opplysninger (som medførte en ikke ubetydelig personvernrisiko), ble det i NOU 1993:22 «Pseudonyme helseregistre» foreslått en radikal endring i måten å organisere helseregistere på. I stedet for å lagre helseopplysinger med fødselsnummer, ble det foreslått at opplysningene skulle lagres under pseudonymer generert av en tiltrodd pseudonymforvalter. Tankegangen og prinsippet var det samme som i PETs-rapporten fra 1995: ved å bytte ut personidentifiserbare identifikatorer med pseudonymer kunne man oppnå samme funksjonalitet, samtidig som risikoen for personvernkrenkelser ble vesentlig redusert.

2 Chaum, «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», Communications of the ACM, vol. 24 no. 2, 1981

1.2 Forsøk på definisjon

Selv om begrepet «personvernøkende teknologi» og akronymet «PETs» er relativt kjent i miljøer som arbeider med personvernspørsmål,[3] finnes det fremdeles ingen omforent definisjon. Kjernen i begrepet har imidlertid hele tiden vært dataminimalitet, nærmere bestemt på å begrense muligheten for å identifisere den opplysningene gjelder. Dette fremkommer av Herbert Burkerts mye siterte definisjon:[4]

> *«The term privacy-enhancing technologies (PETs) refers to technical and organizational concepts that aim at protecting personal identity.»*

Fokuset på identitet kan forklares ved at personverninteresser ikke gjør seg gjeldende dersom den opplysningene gjelder ikke kan identifiseres. Dette faktum gjenspeiles i personopplysningslovgivningen som bare gjelder i den grad det behandles opplysninger om en identifiserbar person.

I personvernkretser har det vært en debatt om kryptografi faller innenfor PETs-begrepet. Uenigheten kan skyldes at kryptografi har mange bruksområder. Benyttes kryptografi som ledd i en anonymiserings- eller pseudonymiseringsprosess, vil dette falle inn under den opprinnelige forståelsen av PETs. Er det snakk om innholdskryptering av opplysninger som kommuniseres eller som er lagret, vil dette være et rent informasjonssikkerhetstiltak. Kryptering har da som siktemål å verne opplysningene fra uautorisert innsyn (konfidensialitet) eller endring (integritet), og angår ikke identitet og muligheten for identifisering. Dette prinsipielle skillet mellom informasjonssikkerhetstiltak og PETs vil bli nærmere kommentert i eksemplet om pseudonyme helseregistre.[5]

Av deler av diskusjonen om PETs kan man få inntrykk av at PETs er avgrenset til å gjelde programvare som kan bidra til å løse personvern- og sikkerhetsutfordringer på Internett. Det er ingen tvil om at Internett medfører

---

3 For eksempel har det siden år 2000 vært avholdt en årlig internasjonal workshop om PETs, se http://petworkshop.org/.

4 Burkert, «Privacy-enhancing technologies: typology, critique, vision», I: Technology and privacy: the new landscape, Agre og Rotenberg (red), 1997

5 Se tilsvarende Burkert, «Privacy-enhancing technologies: typology, critique, vision», I: Technology and privacy: the new landscape, Agre og Rotenberg (red), 1997 s 125: «PETs have to be set apart from data-security technologies. It is one of the merits of the discussion on PETs that the concept of data security has been reclarified as to its limits with regard to privacy protection. Data-security measures seek to render data processing safe regardless of the legitimacy of processing. Data security is a necessary but not a sufficient condition for privacy protection. PETs on the other hand, seek to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned. PETs are therefore closer to the social goals of privacy protection.»

nye trusler som kan avhjelpes med ulike typer tekniske løsninger. Eksempler på dette er brannmurer, antivirus, antispyware, spamfilter osv. Om PETs også skal omfatte slike tekniske tiltak, som gjerne er knyttet til den enkelte brukers personlige utstyr, kan diskuteres. Jeg er av den oppfatning at slike løsninger primært knytter seg til informasjonssikkerhet, og at man med fordel bør forbeholde PETs om tekniske og organisatoriske tiltak som gjelder identitet og identifisering. Et ensidig fokus på brukerstyrte «tools» henleder tanken til at PETs er begrenset til noe som den enkelte bruker kan anvende. Som vi skal se i kapittel 3.2, vil mange av identitetsspørsmålene i forhold til elektronisk kommunikasjon avhenge av tekniske og organisatoriske forhold knyttet til brukerutstyr, «infrastruktur» og kommunikasjonsmotpart (her kalt «tjenesteyter»).

Mens PETs-begrepet altså må anses forholdsvis innarbeidet, dog med varierende meningsinnhold, har viktige deler av forskningen og utviklingen siden begynnelsen av 2000-tallet skjedd innenfor området identitetsforvaltning (engelsk: identity management). Særlig har utviklingen vært drevet frem av store tverrfaglige EU-prosjekter.[6] Personvernøkende identitetsforvaltning tar utgangspunkt i enkeltindividets ulike roller (f eks ansatt, student, kunde, skattebetaler etc). Sentrale aspekter er hvordan man i elektronisk samhandling kan tilpasse identifisering og autentisering til den aktuelle rolle. Dette reiser spørsmål om tildeling av hensiktsmessig identifikator (f eks brukernavn) og autentiseringsmekanisme (f eks passord). I tillegg til fokuset på å holde opplysninger knyttet til ulike roller atskilt, har forskningen også opptatt seg med spørsmålet om muligheten for å autentisere (etablere tilstrekkelig sikkerhet for) andre forhold enn identitet/roller. Ved å autentisere ulike typer egenskaper (betaling, medlemskap, alder, kjønn, etc) vil det være mulig å tilby en lang rekke tjenester uten å knytte dette til noen identitet.[7] Deler av denne forskningen tar altså utgangspunkt i PETs-tankegangen og dens fokus på dataminimalitet.[8] Forskningen innenfor identitetsforvaltning har imidlertid løftet spørsmålene om identitet og identifiserbarhet opp på et nivå hvor man ikke ensidig ser på muligheten for å begrense identifiserbarhet. Vel så viktig er det å stille spørsmål med *hva* (f eks hvilken rolle) som skal identifiseres og å sørge for at dette gjøres på en tilstrekkelig sikker måte (autentisering). Identitetsforvaltningsperspektivet innebærer derfor en mer helhetlig tilnærming til elektronisk samhandling hvor

6 Se f eks EU-prosjektene PRIME, GUIDE, FIDIS, PRIMELIFE og PICOS.

7 Se f eks Brands, Rethinking public key infrastructures and digital certificates: building in privacy, Cambridge, Mass. 2000, løsninger levert av selskapet http://www.credentica.com/ og arbeider av Jan Camenisch, IBM, http://www.zurich.ibm.com/%7Ejca/publications.html.

8 Se f eks Hansen et al., «Privacy-enhancing identity management», Information Security Technical Report, 1, 2004 35-44.

mange av de tradisjonelle PETs-komponentene kan settes sammen til mer brukervennlige løsninger. Se nærmere om dette i kapittel 3.2-3.5.

Parallelt med den akademisk forankrede forskningen har det i IT-industrien skjedd en rivende utvikling av tekniske standarder for identitetsforvaltning.[9] Drivere i dette arbeidet har særlig vært å effektivisere tilgangsstyringen til virksomheters ulike ressurser og tjenester. Bak arbeidet ligger også ønsker om å imøtekomme regulatoriske krav i forhold til informasjonssikkerhet og i forhold til å ha kontroll på hvem som har tilgang til hva. Det er slike standarder som ligger til grunn for felles tilgangsløsninger (single sign-on), slik MinSide og Altinn er eksempler på. Selv om informasjonssikkerhet og personvern er sentrale hensyn ved utvikling av standardene, vil personvernimplikasjonene langt på veg avhenge av *hvordan* disse implementeres.[10] I den forbindelse bør det nevnes at PETs av og til også benyttes om standarder og systemer som gjør det mulig for den behandlingsansvarlige å etterleve personvernlovgivningens krav. Dette er imidlertid langt fra den opprinnelige betydningen av begrepet. Til dette kan det også anføres at teknologi som er personvern*økende* bør være noe utover teknologi som gjør det mulig å behandle opplysninger i henhold til lovens krav. Se nærmere om systemer og standarder for identitetsforvaltning i kapittel 3.6.

Denne korte oversikten viser altså at PETs (og senere personvernøkende identitetsforvaltning) brukes om nokså ulike tekniske og organisatoriske tiltak for å ivareta personvernet. Etter min mening er det i enkelte tilfeller viktig å holde fast ved den opprinnelige betydningen knyttet til identitet og begrenset identifiserbarhet, jf Burkerts definisjon over. Det må likevel fremheves at utover denne opprinnelige snevre betydningen kan begrepet fungere utmerket i forhold til å synliggjøre betydningen av teknologi for å ivareta personvernet. Slik sett kan PETs benyttes om tekniske og organisatoriske systemer som har blitt utviklet med en *intensjon* om å ivareta personvernet.[11] Dette understreker betydingen av personvernspørsmål ikke er noe som kan håndteres til slutt

9 Særlig toneangivende har standardiseringsorganisasjonene Liberty Alliance og OASIS vært i forhold til utvikling av standarder for såkalt føderert identitetsforvaltning.

10 Enkelte forskere har vært kritiske til denne standardutviklingen og hevder at virksomhetenes interesser i å legge til rette for nye forretningsmodeller har fått mer gjennomslag enn hensynet til brukernes personvern. Se f eks Clarke, Identity Management, 2004. Se nærmere om personvernspørsmål i forbindelse med implementering av standarder for føderert identitetsforvaltning i Olsen og Mahler, «Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'», Computer Law & Security Report, 4 & 5, 2007 342-351 & 415-426 og Olsen og Mahler, Identity management & Privacy, Complex, 2007.

11 Se tilsvarende Bygrave, «Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place», Privacy Law & Policy Reporter, 2002 135-137.

når alle designvalg er tatt, men at personvernhensyn må vektlegges i alle trinn i utviklingsprosessen.

1.3 Politisk ønske om å fremme personvernøkende teknologi

Internasjonalt har det i en årrekke vært politisk oppmerksomhet rundt teknologiens rolle som en trussel mot personvernet, men også som en mulig strategi for å sikre personvernet. Til tross for pionervirksomhet i forhold til pseudonyme helseregistre, må det sies at bevisstheten her hjemme i forhold til PETs har vært nokså lav. Norske myndigheter har i liten grad løftet disse spørsmålene opp på dagsorden, og Datatilsynet har i liten grad arbeidet proaktivt i forhold utvikling og anvendelse av teknologi for å sikre personvernet. Enkelte datatilsynsmyndigheter, som f eks datatilsynsmyndigheten i den tyske delstaten Schleswig Holstein, det nederlandske datatilsynet (Registratiekamer), og tilsynsmyndigheten i Ontario, Canada, har utmerket seg med aktivt å forsøke påvirke teknologiutvikling og -anvendelse. Deler av arbeidet kan karakteriseres som en «strategisk entusiasme» til ny teknologi, hvor deltakelse i forskningsprosjekter og aktiv dialog med IT-industrien gjør det mulig å påvirke aktørenes bevissthet om personvernspørsmål. Slikt arbeid krever ressurser og en klar strategi for hvilken rolle tilsynsmyndigheten skal ha. Som vi skal se er dagens lovgivning teknologinøytral og regulerer *anvendelse* av teknologi, og ikke teknologien i seg selv, noe som kan forklare at tilsynsmyndigheter ofte har liten innflytelse på selve teknologiutviklingen. Se nærmere om dette i kapittel 4.

Fra EUs side er det en klar politisk vilje til å fremme PETs. I forbindelse med evaluering av medlemsstatenes implementering av personverndirektivet (95/46/EF) i 2003, ble videre satsning på PETs løftet frem som en av satsningsområdene.[12] Dette er senere fulgt opp fra EU-kommisjonen med en handlingsplan for å fremme PETs.[13] Kommisjonens strategi er for det første å fremme *utvikling* av PETs, legge incentiver for næringslivets og offentlige myndigheters *anvendelse,* samt å heve folk flest sin *bevissthet* om PETs og personvernsspørsmål.

I Norge er spørsmål knyttet til personvern og personvernøkende teknologi berørt i St.meld. nr 17 (2006–2007) («IKT-meldingen»). Av meldingen fremkommer det at Regjeringen ønsker å styrke satsningen på personvernøkende teknologi. Her er PETs beskrevet som «Teknologi som støttar opp

12 EU Commission, First report on the implementation of the Data Protection Directive (95/46/EC), 2003.

13 European Commission, Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs), 2007.

under personvern i elektronisk kommunikasjon over Internett». Dette er en noe unyansert beskrivelse, da PETs som vi skal se ikke bare er relevant i forhold til Internett. Beskrivelsen sier heller ikke noe om *hvordan* teknologien kan styrke personvernet. Kryptering nevnes som eksempel på PETs. Som nevnt over strides det om kryptering er en sikkerhetsteknologi eller PETs. Gode grunner taler i alle fall for at man må skille mellom innholdskryptering og kryptering i forbindelse med anonymisering og pseudonymisering. For øvrig fremhever meldingen viktigheten av at det i samfunnet legges til rette for anonyme eller pseudonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg (kapittel 8.3.3 «Retten til å være anonym»). I den forbindelse nevnes viktige områder som faller inn under kjerneområdet for PETs og identitetsforvaltning:

- *Pseudonyme løysingar som alternativ til full anonymitet og full identifikasjon*
- *Pseudonyme sertifikat i løysinger for digital signatur der dette er tilstrekkeleg*
- *Anonyme betalingskort som alternativ til bankkort/kredittkort som er knytte til identitet.*

Det er naturlig å lese meldingen slik at ønsket om å bevare muligheten for anonymitet nødvendigvis må legge føringer for utvikling og anvendelse av teknologi. Sammenhengen mellom anonymitet/pseudonymitet og PETs/identitetsforvaltning vil bli nærmere belyst i den videre fremstillingen.

2 Pseudonyme helseregistre

Boe-utvalgets forslag til en ny registerform for lagring av helseopplysninger til forsknings- og administrasjonsformål er et godt eksempel på hvordan tekniske og organisatoriske tiltak kan bidra til å sikre personvernet. Som nevnt i innledningen tar registerformen utgangspunkt i selve grunntanken med PETs ved at opplysningene som lagres er knyttet til et pseudonym som ikke direkte kan knyttes til noen identifiserbar person.

Forslaget var nyskapende og dristig, og ble ikke helt uventet møtt med en god del skepsis. Til tross for en noe kronglete lovgivningsprosess,[14] er den

14 Boe, «Nye helseregistre inn bakveien?» Kritisk juss, Årg. 27, nr 1/2, 2000 63-77. http://www.afin.uio.no/forskning/notater/6_00.html.

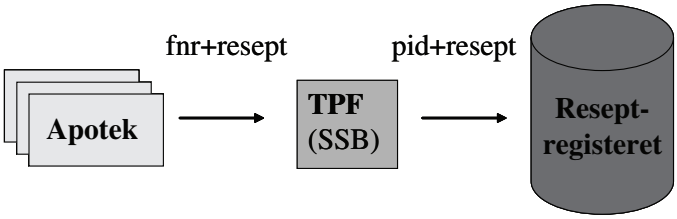
pseudonyme registerformen nå tatt inn i dagens helseregisterlov.[15] Loven skiller i § 2 mellom fire opplysningstyper:

> *helseopplysninger:* taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson,
>
> *avidentifiserte* helseopplysninger: helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet,
>
> *anonyme opplysninger:* opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson,
>
> *pseudonyme helseopplysninger:* helseopplysninger der identitet er kryptert eller skjult på annet vis, men likevel individualisert slik at det lar seg gjøre å følge hver person gjennom helsesystemet uten at identiteten røpes

Et hovedskille går mellom anonyme og avidentifiserte opplysninger, og personidentifiserbare (kalt «helseopplysninger» over) og pseudonyme opplysninger. De to førstnevnte er *ikke personentydige*, det vil si at det ikke er knyttet noen entydig identifikator som gjør det mulig å legge til flere opplysninger på et senere tidspunkt. Dette begrenser muligheten for å forske på denne type data siden man ikke kan følge et individ over tid eller samkjøre dataforekomster angående samme individ fra ulike registre. Personidentifiserbare opplysninger og pseudonyme opplysninger er derimot begge personentydige. Forskjellen er at personidentifiserbare opplysninger er knyttet til identifiserbare opplysninger (typisk fødselsnummer), mens pseudonyme opplysninger er knyttet til et pseudonym som hindrer direkte identifisering av den opplysningene gjelder.

15 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), lov 18. mai 2001 nr 24.

Begrunnelsen for at et pseudonymt register anses å kunne ivareta forskningens behov samtidig som personvernet ivaretas på en hensiktsmessig måte, kan illustreres med informasjonsflyten i det pseudonyme reseptregisteret.[16]



Figur 1 Informasjonsflyt i reseptregisteret

Apotekene registrerer reseptopplysninger og fødselsnummer på rekvirenten. Hver måned sender apotekene disse opplysningene til tiltrodd pseudonymforvalter («TPF» – i dette tilfellet Statistisk sentralbyrå (SSB)). Selve reseptopplysingene er kryptert for TPF. TPF kjører fødselsnumrene gjennom en en-veis krypteringsalgoritme som generer et entydig pseudonym. Pseudonym og tilknyttede reseptopplysninger blir så oversendt til reseptregisteret hvor opplysningene lagres. Siden krypteringsalgoritmen genererer det samme pseudonymet hver gang, vil opplysninger om nye reseptutlevering legges til den enkeltes profil i registeret. Registeret er altså i likhet med et personidentifiserbart register personentydig, noe som gjør det mulig å følge enkeltindivider over tid. Forskjellen er identifikatoren som er knyttet til opplysningene. I et pseudonymt register er fødselsnummer byttet ut med et pseudonym som er generert av en tiltrodd tredjepart. I prinsippet skal derfor et personidentifiserbart og et pseudonymt register være like godt egnet til å oppfylle helseforsknings- og administrasjonsformål. Vi kommer tilbake til innvendingene som har kommet mot dette utgangspunktet rett under.

Fra et personvernsynspunkt er et pseudonymt register å foretrekke fremfor et personidentifiserbart. Poenget med den pseudonyme registerformen er å sikre at de som får tilgang til opplysningene (også autoriserte personer) ikke skal kunne identifisere personen opplysningene omhandler. Risikoen for personvernkrenkelser er derfor vesentlig redusert.

I et personidentifiserbart register vil ivaretakelsen av personvernet i mye større grad avhenge av sikkerhetstiltak og tilgangskontroll. Etter mye diskusjon

16 Registeret er nærmere regulert i Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret), forskrift 17. oktober 2003 nr 1246.

rundt valg av registerform for Norsk pasientregister, falt man ned på et identifiserbart register med «internt krypterte identiteter». I forarbeidene til endring av helseregisterloven ble det argumentert med at personvernet vil bli tilfredsstillende ivaretatt med tradisjonelle sikkerhetstiltak som skal sikre at bare autorisert personell skal ha tilgang til de identifiserbare opplysningene.[17] Med tanke på den etablerte oppfatningen om at den største sikkerhetstrusselen kommer fra virksomheters egne ansatte, kan dette sies å være betenkelig.

Det er altså her den prinsipielle forskjellen mellom den pseudonyme og identifiserbare registerformen ligger: sikkerhetstiltak som «internt krypterte identiteter» sikrer bare mot *uautorisert* tilgang og løser ikke den sårbarheten som ligger i at *autorisert* personell har tilgang til identifiserbare opplysninger. Et pseudonymt register må også vernes mot uautorisert tilgang med tradisjonelle sikkerhetstiltak, men gjør registeret vesentlig mindre sårbart for misbruk fra de som faktisk er autorisert til å behandle opplysningene. Det er dette som gjør at man kan kalle den pseudonyme registerformen for «personvernøkende». Innholdskryptering og tilgangskontroll er bare tradisjonelle sikkerhetstiltak, jf sondringen PETs og sikkerhetsteknologi i kapittel 1.2.

I debatten rundt Norsk pasientregister ble det brukt som argument for et identifiserbart register at den pseudonyme registerformen ikke gir like god datakvalitet som et identifiserbart register og at anvendeligheten er begrenset fordi rettslige og tekniske hindre gjør det umulig å kontakte den opplysningene gjelder. Det er ikke anledning til å gå inn på disse spørsmålene her.[18] Det man kan slå fast er i hvertfall at den pseudonyme registerformen oppfattes som mer kompleks, noe som har gitt grunnlag for forvirring og skepsis fra politikere og helseforskere.[19]

17 Se Ot.prp. nr 49 (2005–2006) Om lov om endringer i helseregisterloven (Norsk pasientregister).

18 Innvendingene har blitt imøtegått av Kompetansesenteret for IT i helsesektoren (KITH) og professorene Dag Wiese Schartum og Erik Boe. Dokumenter er tilgjengelig på nettsiden Personvern på nettet under tittelen «Åpen høring om forslaget til Norsk Pasientregister», 6. november 2006, http://www.personvern.uio.no/pvpn/nyheter.html.

19 Forskningsresultater viser for øvrig at de pseudonyme registerne er velfungerende i praksis, men at det fremdeles hersker en del tvil om hva et pseudonymt register faktisk innebærer. Se nærmere Andresen, «On Pseudonymous Health Registers: While they Work as Intended, they are Still Controversial in Norway», Proceedings of the First International Conference on Health Informatics, Funchal, Madeira - Portugal, Vol 1, 2008 59-66 og L'Abée-Lund, Pseudonymisering av personopplysninger i sentrale helseregistre, Oslo, 2006.

3 Elektronisk kommunikasjon

3.1 Elektroniske spor og identifisering

Personverndebatten både her hjemme og internasjonalt har de senere år vært preget av nye personvernutfordringer knyttet til «elektroniske spor». Elektroniske spor er et bilde på et bredt spekter av opplysninger som typisk genereres og lagres ved bruk av ulike elektroniske hjelpemidler. Studier av personvernproblematikk knyttet til elektroniske spor viser at det siden begynnelsen av 1990-tallet har vært en drastisk økning i mengden elektroniske spor og at disse blir stadig mer innholdsrike.[20] Metodene for å analysere slike data har utviklet seg i takt med den teknologiske utvikling og gjør det mulig å gi et nyansert bilde av gruppers eller enkeltpersoners bevegelsesmønster, omgangskrets og interesser.[21]

Forskningsresultater viser også at utbredelsen av elektroniske tjenester gjør at man som enkeltindivid i stadig større grad og på stadig flere samfunnsområder oppfordres eller tvinges til å identifisere seg.[22] Dette gjelder både for å få tilgang til kommunikasjonstjenester og i forhold til virksomheter som yter innholdstjenester som forutsetter elektronisk kommunikasjon. På visse områder er det klart at det er et legitimt behov for å kunne identifisere den man kommuniserer med eller disponerer rettslig i forhold til. Dette gjelder f eks i forhold til å sørge for at bare autorisert helsepersonell får tilgang til lagrede helseopplysninger, at en medkontrahent kan holdes ansvarlig for kontraktsrettsbrudd, eller at den som gjør seg skyldig i straffbare forhold kan identifiseres og holdes ansvarlig for sine ugjerninger. På andre områder, f eks i forhold til mange av våre dagligdagse trivielle gjøremål, kan det imidlertid tenkes at identifisering er mindre viktig.

Fra et personvernsynspunkt gir hyppigere krav til identifisering grunn til å reise prinsipielle spørsmål knyttet til om identifisering er *nødvendig*, *hva* som eventuelt skal identifiseres og *hvordan* man foretar en identifisering.

---

20 Se Teknologirådet, Elektroniske spor og personvern, 2005 og Norsk Regnesentral, Elektroniske spor, Oslo 2005.

21 Se nærmere om automatisert profilering i Bygrave, Data protection law: approaching its rationale, logic and limits, Dortrecht 2002, s 104–105 og kapittel 17.

22 Se f eks Teknologirådet, Elektroniske spor og personvern, 2005, s 106, Norsk Regnesentral, Elektroniske spor, Oslo 2005, s 65 og Kent og Millett, Who goes there?: authentication through the lens of privacy, Washington, DC 2003, s 30. Se også Datatilsynet, E-forvaltning – Datatilsynets tilrådning til regjeringen, Datatilsynets nettsted, 2007, s 6, hvor tilsynet tilråder regjeringen om at det «trekkes opp retningslinjer som sikrer at identifisering kun skjer når det er reelt behov for sådan».

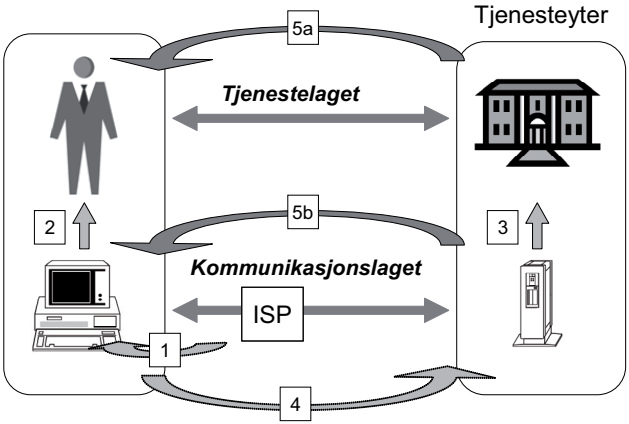
- *Nødvendig* sikter til at det i mange transaksjoner ikke er nødvendig å vite *hvem* man samhandler med. Det man egentlig trenger å vite er f eks om betalingen er mottatt, om vedkommende har betalingsevne og -vilje, alder, kjønn, medlemskap etc.
- *Hva* henspeiler på det faktum at vi alle har ulike roller og at det er den relevante rollen som skal identifiseres, jf introduksjonen til identitetsforvaltning i kapittel 1.2.
- *Hvordan* sikter til at identifiseringen må ha tilstrekkelig kvalitet slik at man f eks unngår forveksling og identitetsmisbruk.

Et sentralt begrep i forhold til disse spørsmålene er *autentisering*. Autentisering er en prosess som tar sikte på å etablere tilstrekkelig sikkerhet for ulike påstander. Påstanden kan f eks knytte seg til hvem man påstår å være eller en bestemt egenskap. F eks kan en påstand om at man er over 18 år understøttes ved å vise gyldig ID-kort i skranken, mens en påstand om at man har rådighet over en bestemt brukerkonto på Internett understøttes av et passord. Se nærmere om autentisering i kapittel 3.5.

I det følgende skal vi se nærmere på hvordan utfordringene knyttet til elektroniske spor, identifisering og autentisering gjør seg gjeldende innenfor identitetsforvaltning på Internett.

3.2 Identitetsforvaltning i tjeneste- og kommunikasjonslag

Det er innen elektronisk kommunikasjon, og spesielt Internett, at det har vært mest fokus på personvernøkende teknologi. Mye av diskusjonen har vært knyttet til enkelte brukerstyrte tekniske løsninger som kan hindre «tjenesteytere» i å opparbeide profiler over brukeres gjøren og laden på Internett. Vi skal her se at dette er én viktig problemstilling, men at det også er andre spørsmål som omhandler identitet og identitetsforvaltning som fortjener oppmerksomhet. Utgangspunktet for den videre fremstillingen er Figur 2 som skiller mellom tjeneste- og kommunikasjonslag og som angir forholdet mellom bruker, ISP og tjenesteyter.



Figur 2 Identitetsforvaltning i tjeneste- og kommunikasjonslag

Modellen er en forenkling av informasjonsflyten mellom en bruker og en tjenesteyter på Internett.[23] Poenget er å synliggjøre at visse identitetsforvaltningsspørsmål kan knyttes til den tekniske infrastrukturen som Internett utgjør (kommunikasjonslaget), mens visse spørsmål må løses i tjenestelaget. Mens kommunikasjonslaget i hovedsak gjelder identifisering og autentisering av maskiner (brukers klient og tjenesteyters server), handler tjenestelaget om identifisering og autentisering av brukeren og tjenesteyteren. Vi skal i det følgende se nærmere på de enkelte relasjonene og hvordan de mest omtalte PETs kan bidra til å sikre personvernet.

3.2.1 Relasjonen ISP – bruker (1) og (2)

For å kunne knytte sin datamaskin til Internett må brukeren for det første inngå avtale med en tilbyder av elektronisk kommunikasjon («ISP», nr 1 i figuren). Tilbyderen har etter ekomforskriften § 6–2, jf ekomloven § 2–8 plikt til å føre oversikt over enhver sluttbrukers navn, adresse og nummer/ adresse for tjenesten. Oversikten skal inneholde opplysninger som gjør det mulig å

23 Modellen tar utgangspunkt i TCP/IP-referansemodellen for Internett og dens lagdeling av protokoller og tjenester. Av figuren kan man få inntrykk av at bruker og tjenesteyter kan kommunisere direkte med hverandre i tjenestelaget. I realiteten går all kommunikasjon gjennom kommunikasjonslaget, men siden visse spørsmål knyttet til identifisering og autentisering ikke løses av kommunikasjonslaget må disse løses på toppen av eksisterende infrastuktur og tjenester. Se nærmere om datanett-teori i Hannemyr, Hva er internett, Oslo 2005, s 57–64 og Tanenbaum, Computer networks, 4th, Upper Saddle River, N.J. 2003, s 37–48.

entydig identifisere de registrerte. Tilbyderen må dermed sørge for å legge til rette for hensiktsmessige rutiner for identifisering og autentisering av sluttbrukere. Dette gjelder særlig der salg av abonnement skjer via mellomledd (kiosker etc) eller via Internett. Kvaliteten på disse rutinene er grunnleggende for datakvaliteten i tilbyders oversikt over sluttbrukere. Dersom abonnementet knyttes til feil person vil følgelig all loggføring av senere trafikkdata være knyttet til feil person. Sett i lys av en eventuell implementering av EUs datalagringsdirektiv 2006/24/EF, og dets krav til tilbydere om lagring av ulike typer transaksjonsopplysinger, er dette spørsmålet om datakvalitet viktig. Se nærmere om registreringsplikten i kapittel 4.1.

Tilbyder har som hovedregel taushetsplikt for lagrede trafikkdata og abonnementsopplysninger, men kan, dersom vilkårene for dette foreligger, utlevere slike opplysninger til politiet og påtalemyndigheten. Reglene om taushetsplikt for tilbyder, og andre som utfører arbeid eller tjeneste for tilbyder, følger av ekomforskriften kapittel 7, jf ekomloven § 2–9. I utgangspunktet er det derfor bare tilbyder som vil ha kjennskap til koblingen mellom bestemte IP-adresser og den sluttbruker som har anvendt IP-adressen. Som vi skal se, har dette betydning for andre aktørers, f eks *tjenesteyteres*, mulighet til å anvende IP-adresser til å identifisere brukere av sine tjenester.

For å sikre at ikke uvedkommende får tilgang til brukerens maskin er det hensiktsmessig at maskinen er satt opp med et tilgangskontrollsystem (nr 2 i figuren). Formålet med tilgangskontrollen vil ikke bare være å sikre at ikke uvedkommende kan tilegne seg de ressurser og tjenester som maskinen gir tilgang til, men også at ikke andre benytter maskinen til handlinger på Internett som brukeren kan risikere å bli konfrontert med, f eks handlinger som kan medføre straff eller erstatningsplikt. En særlig utfordring knytter seg til trådløse nettverk. Dersom brukeren ikke har satt opp tilfredsstillende sikkerhet på sitt trådløse nettverk vil andre, f eks naboer eller andre som befinner seg i nærheten, kunne knytte seg til nettverket og kommunisere på Internett ved hjelp av brukerens abonnement. Tilbyderen av elektronisk kommunikasjon vil normalt ikke kunne skille mellom abonnentens anvendelse av sitt abonnement og andres uautoriserte anvendelse. Alle transaksjonsopplysninger knyttet til abonnementet som loggføres vil dermed i utgangspunktet assosieres med abonnenten. Dette vil kunne ha betydning for bevisbyrden dersom transaksjonsopplysninger lagret hos tilbyderen benyttes i en senere straffesak eller sivil tvist.

3.2.2 Relasjonen bruker – tjenesteyter (3) og (4)

I mange tilfeller vil det være viktig for brukeren å vite hvem han kommuniserer med over Internett. For eksempel vil det være viktig for brukeren å ha

sikkerhet for at den websiden han har lastet ned faktisk tilhører nettbanken eller nettbutikken han ønsker å benytte seg av (nr 4 i figuren). Identifisering og autentisering av et nettsted og dets innehaver bygger på egenskaper ved kommunikasjonslaget, nærmere bestemt koblingen mellom virksomheten og et domenenavn (se nr 3 i figuren). Brukerens mulighet til å vurdere hvilket nettsted han har lastet ned avhenger av egenskaper ved brukerens nettleser, eventuelle sikkerhetstjenester som tilbys av webserveren og av hvordan sikkerhetstjenestene presenteres av nettleseren. Dersom brukeren er sikker på domenenavnet på det aktuelle nettstedet, vil en sjekk av nettstedets URL[24] i adressefeltet på nettleseren gi bekreftelse på at det er korrekt webside. Ytterligere sikkerhet kan oppnås ved bruk av serversertifikater[25] som krypterer kommunikasjonen mellom klient og server. Dette presenteres for brukeren ved at adressefeltet viser «https://». Enkelte nettlesere benytter i tillegg symboler, f eks hengelåssymbol i Internett Explorer, for å indikere at man er på en «sikker» webside med kryptert forbindelse. Et problem knyttet til standard serversertifikater er imidlertid at det tidligere har vært liten eller ingen kontroll med aktøren som har kjøpt tjenesten. Det har derfor ikke vært noe i veien for at serversertifikat har blir satt opp på «falske» nettsider hvor hensikten er å forlede brukeren med hensyn til hvem som faktisk står bak siden. Hvis brukeren da utelukkende bygger sin tillitt på adressefeltets visning av https eller hengelåssymbolet, men ikke sjekker den faktiske URL eller hvem som faktisk har fått sertifikatet utstedt til seg, vil brukeren kunne bli forledet til å utlevere opplysninger til et «utrygt» nettsted – riktignok med en «trygg» forbindelse.[26] Innføringen av EV (Extended Validation) SSL-sertifikater tar sikte på å endre denne situasjonen, hvor man som kjøper av et slikt sertifikat må gjennomgå en godkjenningsprosedyre som skal sikre at den som får sertifikat utstedt til seg er den vedkommende hevder å være og at nettstedet ikke blir brukt til ulovlig virksomhet.[27]

24 URL er forkortelsen for Uniform Resource Locator.

25 SSL (Secure Sockets Layer) og etterfølgeren TLS (Transport Layer Security) er krypteringsprotokoller basert på offentlig-nøkkel infrastruktur (PKI) som sikrer autentisering av server (men ikke klient), samt konfidensialitet og integritet for meldinger mellom klient og server.

26 Selv om brukeren skulle ta seg tid til å sjekke hvem som står som sertifikatinnehaver, er det ikke sikkert at denne informasjonen er egnet til å gi brukeren noen holdepunkter for hvem som står bak nettstedet. Hvis f eks utvikling av nettstedet har vært delegert bort, har det forekommet at dette selskapets navn, og ikke oppdragsgivers navn, har blitt oppført som sertifikatinnehaver. Se nærmere om brukeropplevelsen av serversertifikater i Riisnæs, Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar, Bergen 2007, kapittel 8.4.

27 EV SSL er utviklet av organisasjonen Certification Authority/Browser Forum (CAB Forum), se http://www.cabforum.org/. (sist nedlastet 25.01.2008). Utviklingen har skjedd i nært samarbeid med ledende nettleserprodusenter, som forventes å implementere løsningen blant annet ved bruk av fargekoder for å indikere sikkerhetsnivå nettsteder. Se omtale, Søiland, «Sikrere mot id-tyveri», Computer World, 15.01.2007, sist nedlastet 02.06.2008.

3.2.3 Relasjonen tjenesteyter – bruker (5a) og (5b)

Vi har nå ryddet veien for å ta fatt på den relasjonen som har fått mest oppmerksomhet i personverndebatten, og hvor behovet for PETs blir aktualisert: virksomheters identifisering og autentisering av brukere (nr 5a og 5b i figuren). Ovenfor så vi at virksomhetens domenenavn (som korresponderer med en unik IP-adresse) ble benyttet for å autentisere webservere og bakenforliggende virksomhet. Brukeren vil imidlertid normalt ikke ha en unik IP-adresse som er egnet til å identifisere vedkommende overfor virksomheten, dessuten er kunnskap om koblingen mellom IP-adresse og bruker i utgangspunktet forbeholdt tilbyder av elektronisk kommunikasjon. Identifikasjon av brukeren vil derfor hovedsakelig finne sted i det jeg har kalt *tjenestelaget* (nr 5a i figuren). Utfordringene her knytter seg blant annet til valg av hensiktsmessig identifikator (f eks brukernavn) og autentiseringsmekanisme (f eks passord). Se nærmere om denne *identitetsforvaltningen* i kapittel 3.3 under.

Proxyservere for å undertrykke IP-adresse

Selv om tjenesteyteren normalt vil måtte basere identifisering og autentisering av brukeren på tjenestelaget, er det enkelte personvernmessige utfordringer som knytter seg til kommunikasjonslaget (nr 5b i figuren). Her finner vi også en rekke tekniske tiltak (PETs) som brukeren kan ta initiativ til å anvende for å ivareta sitt personvern.[28] For eksempel vil brukerens IP-adresse være en potensiell mulighet for tjenesteytere til å generere en profil over nettbrukeres bruksmønster. Dette vil særlig kunne være et problem i tilfeller hvor brukeren har en fast IP-adresse,[29] som gjør det mulig for tjenesteyteren å kjenne igjen IP-adressen fra sesjon til sesjon. Dersom brukeren ved en anledning blir identifisert (i tjenestelaget), vil tjenesteyteren i prinsippet kunne knytte denne informasjonen til IP-adressen for fremtidig bruk. Ved senere samhandling vil da brukeren anses som identifisert. Et teknisk tiltak for å avhjelpe disse personvernutfordringene knyttet til IP-adresser er bruk av anonymitets- eller pseudonymitetstjenester som undertrykker brukerens IP-adresse. Slike tjenester bygger på ruting av kommunikasjonen via flere proxyservere, slik at IP-adressen som formidles til tjenesteyter ikke er brukerens reelle adresse. Slike tjenester

28 Se f eks denne oversikten over «Privacy Tools» hos Electronic Privacy Information Center (EPIC), http://epic.org/privacy/tools.html

29 I motsetning til dynamisk IP-adresse hvor brukeren tildeles en ny adresse for hver oppkobling til Internett.

kan også benyttes til anonym publisering som er motstandyktig mot sensur, siden det er vanskelig å avdekke hvor den aktuelle server befinner seg.[30]

Håndtering av informasjonskapsler

En annen personvernmessig utfordring som hører hjemme i kommunikasjonslaget er bruk av informasjonskapsler («cookies»). Protokollen for web, HTTP, er en statusløs protokoll som ikke holder rede på transaksjonshistorikken mellom nettleser og webserver. Dette er et problem ved f eks netthandel hvor det vil være en viktig funksjonalitet å sikre at websiden holder rede på hvilke varer kunden har valgt. Informasjonskapsler er en løsning på dette problemet og gjør det mulig for webserveren å lagre, og senere lese, små tekstfiler på brukerens maskin med blant annet statusinformasjon om den aktuelle eller tidligere sesjoner. Selv om informasjonskapsler slik sett er en nyttig teknologi innebærer den også visse personvernmessige utfordringer. For eksempel gir informasjonskapsler tjenesteytere en potensiell mulighet til å kjenne igjen og danne profiler over brukeres nettbruk på tvers av sesjoner og nettsteder. Særlig gjelder dette for enkelte aktører, f eks leverandører av reklame eller søketjenester, som er representert på mange nettsteder og som kan følge nettbruken fra nettsted til nettsted. I likhet med IP-adresser vil en identifikasjon av brukeren i tjenestelaget i prinsippet gjøre det mulig å knytte identifiserende opplysninger til informasjonskapsler. Det finnes en rekke tekniske tiltak som kan gi brukeren kontroll over de personvernmessige implikasjonen ved informasjonskapsler. I tillegg til at standard nettlesere har funksjonalitet for å gi brukeren kontroll, finnes det software som brukeren kan velge å laste ned («cookie cutters» etc). Se nærmere om den rettslige reguleringen av informasjonskapsler i kapittel 4.1.

Støtte for informerte valg

I tillegg til tekniske løsninger for å undertrykke brukerens IP-adresse og kontrollere informasjonskapsler, har tekniske løsninger for å understøtte brukeren i å foreta informerte valg gjerne blitt omtalt som PETs. P3P (Platform for Privacy Preferences) er den tekniske løsningen som har fått desidert mest oppmerksomhet.[31] Formålet med P3P er å gjøre det enklere for brukeren å forstå nettsteders personvernpolicy. Dersom et nettsted samler inn personopplysninger, vil personvernpolicyen være et naturlig sted å oppfylle lovens forpliktelser til blant annet å oppgi hvem som er behandlingsansvarlig, formålet

30 I dag er TOR-nettverket mest utbredt med flere hundretusen brukere internasjonalt, se http://www.torproject.org/. Se nærmere om slike tjenester i Øverlier, Anonymity, privacy and hidden services, Oslo 2007.

31 Se http://www.w3.org/P3P/

med behandlingen, hvilke opplysninger som samles inn, om opplysingene videresendes til andre etc. Det har vist seg at dersom en virksomhet tar seg bryet med å utforme en slik policy er den gjerne i en vanskelig tilgjengelig form som få brukere har forutsetninger for å forstå. P3P gjør det mulig for virksomheten å uttrykke personvernpolicyen på tre nivåer: en kort og standardisert policy, en full policy og en maskinlesbar policy. Brukeren på sin side må benytte en nettleser som støtter P3P (f eks Internett Explorer), og stille inn nettleseren på ønsket personvernnivå før han kan surfe rundt på nettet. Så lenge de besøkte nettstedene har en P3P-personvernpolicy i overensstemmelse med brukerens angitte personvernnivå, vil brukeren ikke merke noe til P3P. Men dersom det ikke er match mellom brukers nivå og virksomhetens policy, vil brukeren bli gjort oppmerksom på det og få mulighet til å lese virksomhetens standardiserte policy i kort- eller fullt format. Mens det tidligere var stor entusiasme og forhåpninger knyttet til P3P, spesielt fra deler av IT-industrien, er det i dag en utbredt oppfatning om at P3P har sine begrensninger. Det er i hovedsak brukerrettede nettsteder tilknyttet store internasjonale selskaper som benytter teknologien, få brukere er kjent med den, og det er ingen garantier for at det som uttrykkes i slike policyer faktisk er korrekt eller overholdes i virksomheten.[32] P3P har i dag størst praktisk betydning i forhold til å automatisk godkjenne eller hindre lagring av informasjonskapsler.[33]

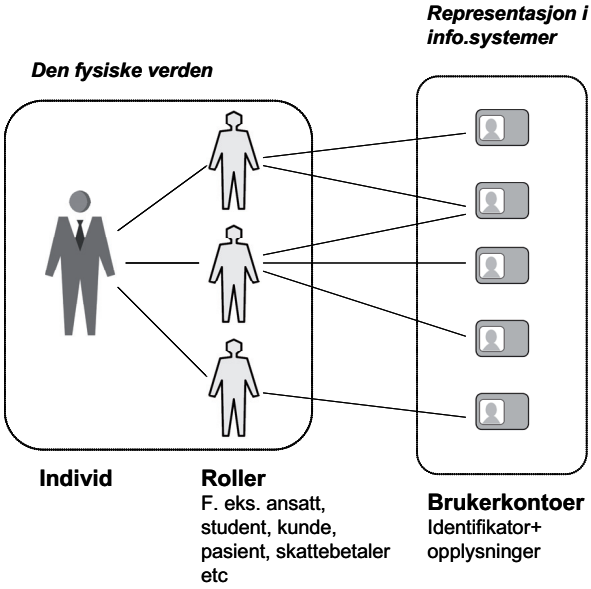
3.3 Nærmere om «identitet» og identitetsforvaltning

Som avsnittet over viser dukker spørsmålet om identitet og identitetsforvaltning opp i flere relasjoner. Her skal vi se nærmere på relasjonen mellom brukeren og tjenesteyteren (5a) i figuren. Hva mener vi egentlig med «identitet» og hvordan kan tjenesteyteren få etablert tilstrekkelig sannsynlighet for at brukeren er den han hevder å være?

32 Det skal nevnes at det også er blitt forsket på tekniske løsninger som gjør det mulig å angi detaljerte regler for hvordan lagrede personopplysninger skal behandles. IBM har f. eks. utviklet EPAL (Enterprise Privacy Authorisation Language) som bygger på forutsetning om at alle personopplysninger i en virksomhet tagges med metadata, og det angis regler for hvem, som for hvilket formål og under hvilke forutsetninger, kan behandle opplysningene. Tilnærmingen har en viss sammenheng med P3P. Begge bygger på bruk av XML-baserte regelsett, og man har sett for seg at det som uttrykkes utad om virksomhetens behandling av personopplysninger gjennom P3P kan håndheves internt gjennom EPAL. Se http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/.

33 Her kan det sondres mellom informasjonskapsler som faktisk er fra nettstedet man besøker, informasjonskapsler fra tredjeparter (f eks fra reklamebannere) og informasjonskapsler fra sider som benytter/ikke benytter P3P.

Identitet er et sammensatt og komplekst begrep. I forhold til elektronisk samhandling kan det være nyttig å sondre mellom individet og individets ulike roller i den fysiske verden og representasjon i form av brukerkontoer i informasjonssystemer. Se figur 3.



Figur 3 Individ, roller og brukerkontoer

For så vidt kan begrepet «identitet» benyttes om alle de tre nivåene (individ, roller og brukerkontoer) i figur 3. I tilegg kan begrepet benyttes både om selve brukerkontoen og om identifikatoren (f eks brukernavnet) som skiller brukerens brukerkonto fra andre brukerkontoer. For å unngå misforståelser er det derfor viktig å presisere hva man mener med identiet. Dette gjelder ikke minst i spørsmål knyttet til såkalt «identitetstyveri».

Erkjennelsen av at man som samfunnsborger daglig veksler mellom ulike roller er viktig for å kunne legge til rette for tekniske løsninger som er hensiktsmessige og forsvarlige fra et personvernsynspunkt. For eksempel vil det kunne være stor forskjell på hvilke opplysninger som vil være relevante og som det vil være ønskelig å dele med familie, venner, lærested, arbeidsgiver, helsevesen, forsikringsselskap, skattevesen eller Internett- og telefonleverandør. Utviklingen i retningen av økt elektronisk samhandling skaper utfordringer

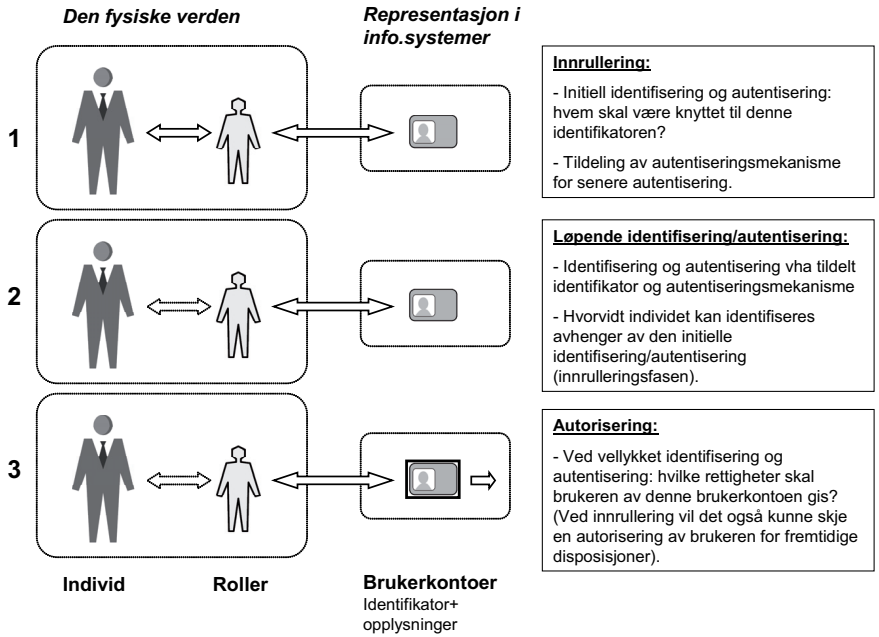
i forhold til å tilpasse identifisering og autentisering til den aktuelle rolle og relasjon.

> *Et eksempel er dagens bruk av e-post. For mange arbeidstakere og studenter utgjør e-postadressen de har fått tildelt av arbeidsgiver eller lærested en viktig kommunikasjonskanal. Det er blitt vanlig å benytte denne e-postadressen ikke bare i forhold til jobb eller studier, men også til fortrolig kommunikasjon med familie og venner, og gjerne også offentlig etater og kommersielle aktører. E-postadressen, som i utgangspunktet er ment å bli brukt til jobbrelatert kommunikasjon, blir på denne måten også benyttet i mange sammenhenger hvor rollen som ansatt eller student er helt uvesentlig, men hvor det er vedkommendes rolle som familiemedlem, venn, borger eller kunde som er det sentrale. Det er nok flere grunner til at mange velger å benytte e-postadressen til mange formål som ikke er relatert til vedkommendes arbeidsoppgaver. For det første kan det gjerne oppleves som tungvint å benytte flere e-postadresser da dette med normalt medfører at man må holde seg à jour med flere e-postadresser. For det andre har det i mange tilfeller ikke vært noe i veien for å benytte e-postadressen til annet enn jobb/studierelatert kommunikasjon. Samtidig har skillet mellom arbeid og fritid gradvis blitt visket ut – noe som også kan forklare hvorfor jobbrelatert e-postadresser også blir benyttet til andre formål. Spørsmålet om arbeidsgivers innsynsrett i arbeidstakers e-post har av Datatilsynet, domstolene og lovgiver tatt utgangspunkt i skillet mellom privat e-post (som arbeidsgiver i utgangspunktet ikke har hatt innsynrett i), og virksomhetsrelatert e-post (hvor utgangspunktet har vært rett til innsyn). Skillet mellom privat og virksomhetsrelatert har i praksis vist seg å være vanskelig å trekke opp. Hadde det vært lagt bedre til rette for at arbeidstakere enkelt kunne bytte fra en rolle til en annen ville antakelig denne problemstillingen ikke vært like aktuell. Det kunne da stilles krav til at arbeidstakere benyttet denne muligheten, noe som ville sikre at det allerede ved utsendelse og mottak av e-post ble skilt jobbrelatert og annen «privat» kommunikasjon. Et eventuelt innsyn av arbeidsgiver ville da være med utgangspunkt i det som allerede fremstår som virksomhetsrelatert e-post. Dette ville i så fall være vesentligere enklere og mer personvernvennlig enn det som har vært tilfellet tidligere: gjennomgang og sortering av all e-post.*

I det følgende skal vi se nærmere på identitetsforvaltningens grunnleggende faser. Som vi skal se, avhenger de personvernmessige aspektene særlig av valg av identifikator og autentiseringsmekanisme.

3.4 Sentrale faser

Identitetsforvaltning kan, som illustrert i Figur 4, brytes opp i tre grunnleggende faser: innrullering, løpende autentisering og autorisering.



Figur 4 Faser

Nærmere om de enkelte fasene:

(1) Innrullering

I innrulleringsfasen er det gjerne fire spørsmål som må adresseres:

- Med hvilken grad av sikkerhet trenger man å vite *hvem* som innrulleres? Trenger man å vite hvem brukeren er? Hvis ja, hvordan etablere tilstrekkelig sikkerhet for at brukeren er den han hevder å være (autentisering)?
- Hvilken *identifikator* skal være knyttet til denne brukeren? (f eks brukernavn)
- Hva slags *autentiseringsmekanisme* skal brukeren utstyres med? (f eks passord)
- Hva skal denne brukeren eventuelt være *autorisert* til å foreta seg i systemet?

(2) Løpende identifisering og autentisering

Når brukeren vender tilbake for å benytte tjenesten, må det skilles mellom to prosesser:

- Identifisering: brukeren individualiseres blant andre lagrede brukere på bakgrunn av identifikatoren som oppgis (f eks brukernavn)
- Autentisering: brukeren benytter autentiseringsmekanismen som bekrefter at han/hun er den som fikk utdelt identifikatoren.

Merk at resultatet av disse to prosessene ikke nødvendigvis medfører at systemet har avdekket *hvem* brukeren er (i betydningen personens alminnelige brukte navn eller identifikator). Hva man vet om brukeren etter vellykket identifisering og autentisering avhenger av innrulleringsfasen og kvaliteten på identifiserings og autentiseringsprosessene der. Dersom det ikke ble foretatt noen autentisering av brukeren i innrulleringsfasen, vil resultatet her simpelthen være at man har en viss grad av sikkerhet for at det er den samme brukeren som nå har logget inn.

(3) Autorisering

Dersom den løpende identifiseringen og autentiseringen er vellykket er spørsmålet hvilke ressurser og tjenester brukeren skal ha tilgang til (autorisering).

3.5 Nærmere om autentisering

I gjennomgangen av fasene over kan man få inntrykk at autentisering bare knytter seg til å etablere tilstrekkelig sikkerhet i forhold til identitet. Det er imidlertid også andre forhold det kan være viktig å etablere sikkerhet om. I mange tilfeller er ikke nødvendigvis identitet så interessant i forhold avgjørelser om å gi eller nekte tilgang til en tjeneste eller ressurs. Man kan skille mellom autentisering av:

- Identitet (i betydningen personidentifiserende opplysninger som f eks navn, adresse og fødselsnummer)
- Rolle (trenger ikke nødvendigvis vite hvem personen er, så lenge man kan få bekreftet at det er en person som oppfyller den relevante rollen som f eks student, ansatt, kunde, ukjent individ men samme som innrullerte tidligere etc)
- Attributt (egenskaper som alder, kjønn, betalingsevne og -vilje etc)

Ved tradisjonelle kommunikasjonsformer vil det ofte være mulig å fysisk observere den identitet, rolle eller egenskap som påberopes. Hvis en godt voksen person ønsker å kjøpe kinobillett til en forstilling med 7-årsgrense, ville det

vekke oppsikt om kassadamen ba om ID-kort for å sjekke personens alder. Dersom hun mot formodning skulle be om ID- kort, ville autentiseringen bygge på følgende premisser: -Er dette et ID-kort som ser ekte ut og som er utdelt etter en tilfredsstillende identitetsautentisering? -Er personen den samme som er avbildet på kortet? Normalt vil kontantbetalingen også godtas også uten forespørsel om *hvem* personen er. I dette tilfellet kan kassadamen fysisk observere alder og kontanter – egenskapene er det man kan kalle *selvautentiserende*.[34]

Ved elektronisk kommunikasjon er utgangspunktet at vi ikke kan basere oss på slik selvautentisering hvor egenskaper kan sanses eller observeres. Opplysninger som kan underbygge påstanden må da kommuniseres av den enkelte, eller av andre som har tilgang til slike opplysninger. Dersom billetten skulle kjøpes på nettet, ville det normale forløpet være at personens identitet ble kjent i forbindelse med gjennomføring av betalingen og at opplysninger om personens billettkjøp blir lagret.

Spørsmålet er så *hvordan* man autentiserer over elektronisk kommunikasjon. Det skjelnes gjerne mellom fire ulike mekanismer for autentisering, nemlig noe man:

- *er* (biometriske kjennetegn),
- *vet* (f eks passord) og/eller
- *har* (f eks smartkort, kortleser, informasjonskapsel, mobilnummer, postforsendelse til folkeregistrert adresse etc).
- *gjør* (f eks karakteristika som trykk, hastighet og bevegelsesmønster når man påfører en signatur)

Enkelte av autentiseringsmekanismene, f eks biometri, reiser nye personvernspørsmål som det ikke er anledning til å ta opp her. Budskapet i denne sammenheng er at man fra et personvernsynspunkt bør gå vekk fra betraktningen om at identifisering handler om å avdekke den enkeltes «sanne» identitet. I enkelte tilfeller er identitet irrelevant, i stedet bør det legges til rette for å autentisere den rolle eller egenskap som er av interesse.[35]

34 Se Lessig, Code: version 2.0, New York 2006, s 40.

35 Et interessant eksempel er eBay og enkelte andre e-handelsplatformer som har hatt suksess med omdømmesystemer for å formidle informasjon om selgere og kjøpere. I slike systemer er det aktørenes opparbeidede omdømme som er det sentrale, ikke identitet. Se nærmere Mahler og Olsen, «Reputation Systems and Data Protection Law», I: eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, Cunningham og Cunningham (red), 2004.

3.6 Systemer og standarder for identitetsforvaltning

Utviklingen i retning av stadig mer elektronisk samhandling med et økende antall relasjoner, medfører et behov for systemer og løsninger for identitetsforvaltning.

Fra den enkelte *brukers perspektiv* handler identitetsforvaltning om håndtering av ulike «brukerkontoer». Rent praktisk vil det si håndtering av et økende antall korresponderende identifikatorer og autentiseringsmekanismer (passord, smartkort, digitale sertifikater etc). Fra brukerens synspunkt er dette en reell utfordring, noe som kan føre til at enkelte skriver ned passordene eller velger det samme passordet flere steder. Fra et sikkerhets- og personvernperspektiv er dette uheldig. En brukerstyrt teknisk løsning på denne utfordringen er f eks å finne i standard nettlesere hvor brukeren kan velge å bli assistert i å knytte brukernavn og passord til rett nettsted.

Fra *virksomheters perspektiv* dreier identitetsforvaltning seg om tildeling og vedlikehold av brukerkontoer. Dette inkluderer, som nevnt i kapittel 3.4, innrullering, løpende identifisering/autentisering og autorisering av brukere. Tradisjonelt har dette vært løst av virksomhetene selv, gjerne med én særegen løsning for hvert system. Mange virksomheter har erfart at det kan være en ressurskrevende oppgave å drifte mange systemer med ulike påloggingsløsninger. Dette kan lett medføre dårlig oversikt over eksisterende brukerkontoer, og brukerne må forholde seg til mange brukernavn og passord. Identitetsforvaltning handler derfor om hvordan man kan effektivisere de aktuelle arbeidsprosessene, blant annet ved å legge til rette for felles tilgangssystemer (single sign-on) hvor én innlogging gir tilgang til flere systemer og tjenester. Med utgangspunkt i åpne tekniske standarder er det nå mulig å implementere identitetsforvaltningsløsninger som ikke bare gjelder virksomhetens egne ansatte, men som også omfatter kunder og samarbeidspartnere. Nye e-forvaltningsløsninger som MinSide er et eksempel på dette, hvor borgerne kan velge mellom flere måter å autentisere seg på (flere alternative identitetstilbydere), og hvor en vellykket autentisering gir tilgang til nett-tjenestene til flere uavhengige statlige og kommunale etater.

Nye identitetsforvaltningsløsninger gir altså muligheter for nye forretningsmodeller og e-forvaltningsløsninger ved at sentrale arbeidsprosesser knyttet til innrullering og løpende identifisering/autentisering kan delegeres til aktører som har spesialisert seg på dette. Hva brukeren skal få tilgang til (autorisering), blir som oftest besluttet lokalt etter en vellykket autentisering av en ekstern identitetstilbyder (f eks BankID). I utgangspunktet må det forventes at personvernet og informasjonssikkerheten blir bedre ivaretatt når profesjonelle identitetstilbydere tar hånd om deler av identitetsforvaltningen, enn om f eks hver enkelt statlige og kommunale etat skulle drifte sine egne løsninger. Det

er også opplagt at felles tilgangsløsninger som MinSide gjør det mulig å tilby samfunnsnyttige tjenester, men også tjenester som direkte kan gavne personvernet, f eks ved å gi innsyn i hvilke opplysninger de enkelte etatene har om den enkelte borger. Det skal imidlertid ikke legges skjul på at utviklingen reiser prinsipielle personvernspørsmål. Tradisjonelt har virksomhetsgrenser vært en av de viktigste barrierene for ivaretakelse av personvernet: ved å holde relasjoner og kontekster atskilt har man kunnet unngå enkeltaktører som «vet alt» om den enkelte borger. Spissformulert kan man si det slik at løsninger for identitetsforvaltning tar sikte på å bryte ned slike barrierer og gjøre opplysninger tilgjengelige på tvers av system- og virksomhetsgrenser. Riktignok tar løsningene gjerne utgangspunkt i at det bare er brukeren selv som skal ha fordelen av å kunne få enkel tilgang til de ulike tjenester, og at opplysningene fremdeles skal være lagret hos den enkelte virksomhet. Dette er imidlertid ingen garanti for at løsningene ikke vil kunne være sårbare for misbruk og legge til rette for utveksling av personopplysninger som ellers ikke ville blitt utvekslet.[36] Et annet aspekt som bør synliggjøres er at identitetsforvaltningsløsninger tar sikte på å tilby en sømløs og brukervennlig brukeropplevelse på tvers av virksomhetsgrenser. Dette hensynet kan i noen tilfeller komme i konflikt med personvernhensyn, hvor prinsippet om brukermedvirkning og kontroll tilsier at brukeren skal være i stand til å vurdere implikasjonene ved å benytte en tjeneste. Dette fordrer at aktørene er sine roller og oppgaver bevisst og at informasjon om disse forhold formidles til brukeren på en hensiktsmessig måte.[37]

36 Et eksempel på en kommersiell løsning som hadde åpenbare personvernsvakheter var Microsoft .NET Passport. Tjenesten tok utgangspunkt i Microsoft sin Hotmail-tjeneste (e-post), hvor innlogging her gav anledning til single sign-on hos f eks eBay og andre store kommersielle aktører. Etter kritikk fra Artikkel 29-arbeidsgruppen (rådgivende arbeidsgruppe bestående av representanter fra datatilsynsmyndighetene i EU-landene), endret Microsoft i 2003 tjenesten til kun å gjelde egne tjenester. I tillegg til kritikk for selve implementasjonen (måten samtykke ble innhentet på, manglende informasjon, uklare ansvarsforhold etc) var arbeidsgruppen kritisk til den tekniske arkitekturen som innebar Microsoft selv som eneste identitetstilbyder og bruk av en unik identifikator for hver bruker. Arkitekturen var sårbar for misbruk siden Microsoft satt på mye informasjon om bruken av tjenesten, og hvor kun avtalemessige forhold hindret tjenesteyterne fra å slå sammen informasjon om felles kunder. Se nærmere om dette i Olsen og Mahler, «Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'», Computer Law & Security Report, 4 & 5, 2007 342-351 & 415-426.

37 Se nærmere om roller og oppgaver og om oppfyllelse av informasjonsplikten etter personopplysingslovgivningen i Olsen og Mahler, «Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'», Computer Law & Security Report, 4 & 5, 2007 342-351 & 415-426 og Olsen og Mahler, Identity management & Privacy, Complex, 2007.

4 Personopplysningslovgivningen

Fremstillingen har så langt gitt en oversikt over de personvernmessige aspektene knyttet til personvernøkende teknologi og identitetsforvaltning. Når fokuset nå rettes over på det rettslige vernet om personopplysninger er hensikten å kortfattet synliggjøre enkelte sammenhenger mellom juss og teknologi. Dette gjelder for det første i hvilken grad personopplysningslovgivningen stiller krav til teknologien (kapittel 4.1). For det andre forholdet mellom enkelte av personopplysningsrettens grunnleggende prinsipper og PETs/identitetsforvaltning (kapittel 4.2).

4.1 Hva reguleres?

Personopplysningsloven (pol) er den sentrale loven på området. Loven gjennomfører Norges forpliktelser etter personverndirektivet 95/46/EF og gjelder for «behandling av personopplysninger». Dette betyr at loven kun gjelder i den grad opplysninger kan knyttes til en identifiserbar enkeltperson. Loven retter seg mot den «behandlingsansvarlige», det vil si den som bestemmer formål og virkemidler for behandlingen. Den behandlingsansvarlige må således følge visse materielle og prosessuelle krav for at behandlingen skal være lovlig.

Personopplysningsloven stiller i utgangspunktet ikke direkte krav til teknologien. Det som reguleres er den behandlingsansvarliges behandling av personopplysninger. Loven sier altså ingen ting direkte om hvordan ny teknologi skal utvikles eller hvordan tekniske standarder skal utformes. Det er først når teknologien *anvendes* av en behandlingsansvarlig for å behandle personopplysninger at de rettslige kravene gjør seg gjeldende. I utgangspunktet gir det derfor ikke mening å snakke om «godkjente» produkter, systemer eller standarder. Ikke overraskende vil det være lettere å overholde personopplysningslovgivningen dersom man har tatt hensyn til personverninteresser og lovens krav ved utvikling av teknologien. Det avgjørende i følge loven er imidlertid hvordan teknologien implementeres og anvendes av den behandlingsansvarlige. Dersom den behandlingsansvarlige velger å delegere bort hele eller deler av behandlingen til en databehandler, er lovens system at det fremdeles er den behandlingsansvarlige som har ansvaret for at lovens regler følges. Det er grunn til å tro at det hersker en utbredt misoppfatning om at man kan overholde personopplysingsloven ved å kjøpe en fiks ferdig teknisk løsning, eller ved å delegere bort behandlingen til en profesjonell aktør. Gode tekniske løsninger og kompetente samarbeidspartnere er vel og bra, men den behandlingsansvarlige sitter altså fremdeles med hovedansvaret.

I forhold til spørsmål om personvernøkende teknologi og identitetsforvaltning finnes også sentrale bestemmelser i lov og forskrift om elektronisk

kommunikasjon (ekomloven og -forskriften). Bestemmelsene retter seg primært mot tilbyder av elektronisk kommunikasjonsnett eller -tjeneste, det vil si aktører som enten gir tilgang til elektronisk kommunikasjon (herunder telefonitjenester og Internett), eller som overfører signaler for slike tjenester. Som nevnt i kapittel 3.2 har tilbyderen etter ekomforskriften § 6–2, jf ekomloven § 2–8 plikt til å føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjenesten. Oversikten skal inneholde opplysninger som gjør det mulig å entydig identifisere de registrerte. Selv om lov og forskrift ikke sier det direkte, må det antas at det implisitt i registreringsplikten er et krav om autentisering av sluttbrukeres identitet ved tegning av abonnement. Hvis ikke vil abonnentopplysningene riktignok kunne entydig identifisere den registrerte, men man vil ikke ha noen sikkerhet for at det er rett person. I praksis har det vist seg at tilbyderne av elektronisk kommunikasjon har hatt problemer med å oppfylle registreringsplikten på en tilfredsstillende måte.[38] Dette kan for det første skyldes ønsket om å gjøre tegning av abonnement så enkelt som mulig, f eks over Internett eller i kiosken på hjørnet. For det andre skyldes det en lav kollektiv bevissthet om skillet mellom identifisering og autentisering. Fødselsnummer er en personentydig identifikator som er godt egnet til identifisering ved at den individualiserer ett individ fra alle de andre. Fødselsnummer skal imidlertid ikke benyttes til autentisering. Fødselsnummeret er nemlig ingen hemmelighet som gir sikkerhet for at den aktuelle personen er den han hevder å være. Dersom man har anledning til å benytte fødselsnummer som identifikator, jf pol § 12, må det derfor i tillegg benyttes en eller flere autentiseringsmekanismer som gir sikkerhet for at et fødselsnummer faktisk er knyttet til den aktuelle personen, jf kapittel 3.5 over.

Ekomloven med forskrift innholder også andre viktige bestemmelser som har betydning for personvernet, blant annet regler om «kommunikasjonsvern mv» (ekomforskriften kapittel 7). Dette omfatter blant annet taushetsplikt og regler om behandling av trafikk- og lokasjonsdata. Som nevnt i kapittel 3.2 har det i personvernkretser vært mye fokus på informasjonskapsler og de muligheter denne teknologien gir til å samle informasjon om internettbrukere på tvers av nettsteder og sesjoner. Faktisk er informasjonskapsler regulert i ekomforskriften § 7–3, hvor utgangspunktet er at det er *forbudt* å benytte informasjonskapsler «uten at bruker er gitt informasjon av den behandlingsansvarlige i henhold til personopplysningsloven, herunder om behandlingsformålet og er

38 Sommeren 2007 ble f eks nett-tjenesten til Tele2 benyttet til å hente ned fødselsnummer, navn , adresse og kredittverdighet for 60 tusen personer. Se omtale i Hannemyr, «Feil nummerbruk», Lov&Data, 92, 2007 29-30. Se også Olsen, «Lovgivningsprosessen bak registreringsplikt for kontantkort til mobiltelefon», Lov & Data, 85, 2006 1-6.

gitt anledning til å motsette seg behandlingen.» Forbudet gjelder likevel ikke dersom det gjelder «teknisk lagring» utelukkende for det formål å overføre eller lette overføringen, eller dersom slik lagring eller adgang til opplysninger er «nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel». Bestemmelsen er oppsiktsvekkende. Den retter seg for det første ikke primært mot *tilbydere* slik loven og forskriften ellers gjør, men til «*tjenesteytere*» som benytter informasjonskapsler (jf skillet mellom ISP og tjenesteytere i Figur 2). For det andre er det et forsøk på rettslig regulering av et spørsmål av svært praktisk karakter hvor gjennomføringen av informasjonsplikten nødvendigvis må skje gjennom tekniske tiltak. I praksis er nok denne bestemmelsen relativt ukjent for pliktsubjektene, og brukerne må sies å være best stilt ved å stole på de tekniske hjelpemidler de har til rådighet for å kontrollere lagring og lesning av informasjonskapsler, jf kapittel 3.2. Bestemmelsen står dessuten i sterk kontrast til personvernregelverket ellers, som gjennomgående er teknologinøytralt. Generelt kan det sies at personvernbestemmelsene i ekomloven og ekomforskriften er viktige, men at de er godt gjemt i et regelverk som primært angir konkurranseregler innenfor elektronisk kommunikasjon.

4.2 Grunnleggende personvernprinsipper

Personvernopplysningsretten kan uttrykkes gjennom noen grunnleggende prinsipper som gjelder for all behandling av personopplysninger. De grunnleggende prinsippene kan sies å være selve kjernen i internasjonal og nasjonal personvernregulering. Hvert prinsipp representerer således et sett med mer detaljerte regler som skal ivareta et nærmere bestemt hensyn eller en regulatorisk strategi som anses hensiktsmessig for å ivareta personvernet i forbindelse med behandling av personopplysninger. Prinsippene kan skisseres på følgende måte:

Rettmessig og rettferdig behandling: All behandling av personopplysninger krever rettslig grunnlag, og den behandlingsansvarlige skal ta tilbørlig hensyn til den registrertes berettigede personverninteresser. Sensitive personopplysninger er underlagt strengere vern enn alminnelige personopplysninger.

Brukermedvirkning og kontroll: Den behandlingsansvarlige skal gjøre behandlingen transparent og forståelig for den registrerte, slik at denne gjøres i stand til å overskue behandlingens konsekvenser og er i stand til å ivareta sine personverninteresser.

Formålsbestemthet: Den behandlingsansvarlige skal før innsamling og behandling av personopplysninger angi et klart og uttrykkelig formål med behandlingen. Opplysningene skal ikke senere benyttes for uforenlige formål.

Minimalitet: Personopplysninger bare skal innhentes, lagres og behandles i den grad de er nødvendige for å oppnå formålet med behandlingen av opplysningene.

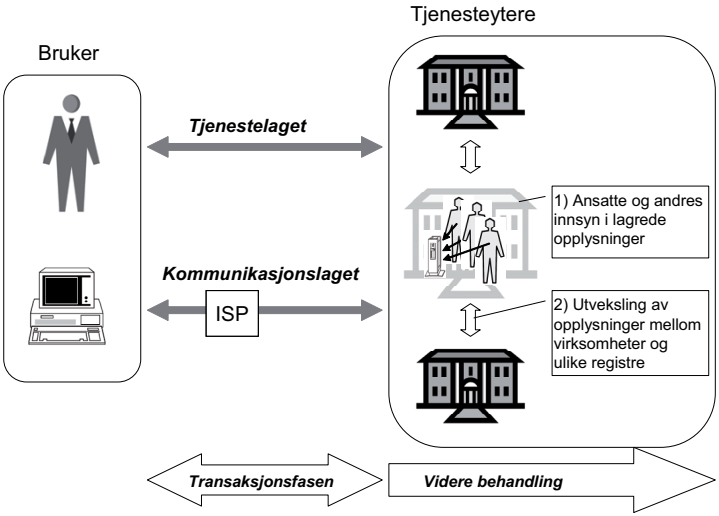
Datakvalitet: Personopplysninger skal ha tilstrekkelig kvalitet i forhold til det formålet de skal anvendes til. Dette innebærer blant annet at opplysningene skal være tilstrekkelig oppdaterte, presise og relevante sett opp mot formålet med behandlingen.

Informasjonssikkerhet: Den behandlingsansvarlige (og databehandleren) skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

De personvernutfordringene PETs og identitetsforvaltning (se kapittel 2 og 3) tar sikte på å løse eller avhjelpe, kan først og fremst knyttes til prinsippene om brukermedvirkning og kontroll, minimalitet og datakvalitet. Vi skal her se nærmere på sammenhengen mellom disse prinsippene og PETs/identitetsforvaltning.

4.2.1 Brukermedvirkning og kontroll

Prinsippet om brukermedvirkning og kontroll kommer til uttrykk i personvernlovgivningens bestemmelser som skal sikre transparens, det vil si bestemmelser om samtykke som behandlingsgrunnlag, informasjonsplikt, innsynsrett og meldeplikt. Gjennomgangen av P3P viser at det finnes tekniske løsninger for å støtte opp under formidlingen av såkalte personvernpolicyer. Videre har vi sett at autentiserings- og identitetsforvaltningsløsninger gjør det mulig å gjennomføre innsynsretten på en mer effektiv måte. Brukermedvirkning og kontroll handler også om at brukeren skal kunne ha kontroll på utlevering og videre behandling av egne personopplysninger. Et grunnleggende skille er derfor mellom «transaksjonsfasen» hvor brukeren kan velge å utlevere opplysninger, og «videre behandling» hvor opplysninger om brukeren er blitt utlevert. Når opplysninger først er blitt utlevert har brukeren liten eller ingen kontroll på behandlingen. Fra et personvernsynspunkt er det da særlig to spørsmål som gjør seg gjeldende: (1) hvem i virksomheten skal ha tilgang til opplysningene; og (2) i hvilken grad kan opplysninger utveksles mellom virksomheter og ulike registre. Skillet mellom transaksjonsfasen og videre behandling illustreres i Figur 5.



Figur 5 Transaksjonsfase og videre behandling

Som vi så av gjennomgangen i kapittel 3.2, kan det være hensiktsmessig å skille mellom identitetsforvaltning i kommunikasjons- og tjenestelaget. Begge disse lagene knytter seg til transaksjonsfasen i figuren. Som nevnt har de klassiske PETs tatt sikte på å gi brukeren kontroll over potensielt identifiserende opplysninger i kommunikasjonslaget (f eks proxy-servere eller «cookie-cutters» for å undertrykke IP-adresse eller informasjonskapsler).

4.2.2 Prinsippene minimalitet og datakvalitet

Som vi har sett har PETs tradisjonelt vært sett på som tekniske og organisatoriske tiltak som tar sikte på å kontrollere adgangen til å identifisere den opplysningene gjelder. Også på det rettslige og politiske planet er minimalitet og anonymitet viet stor oppmerksomhet – dog med litt forskjellige innfallsvinkler. Viktigheten av anonymitet fremkommer for det første av en rekke internasjonale rekommandasjoner angående Internett og autentiseringsløsninger.[39] Her hjemme har spørsmålet om anonymitet særlig vært synliggjort av Datatilsynet som i tilknytning til bompengeringene har fremhevet viktigheten av å kunne *ferdes* anonymt. I personvernteori legges av og til prinsippet til grunn for en

39 Se f eks Artikkel 29-gruppens rekommendasjoner om anonymitet på Internett (WP 6/1997) og autentiseringstjenester (WP 68/2001).

rett til anonymitet eller et eget *prinsipp* om anonymitet.[40] Også i regjeringens IKT-politikk fremheves «at det fremdeles må være tilbud om anonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg.»[41]

Gjeldende lovgivning står imidlertid etter min mening i en klar kontrast til de nevnte uttalelsene om viktigheten av anonymitet. Prinsippet kan skimtes i personopplysningsloven § 11 d) som stiller krav til at opplysninger er «tilstrekkelige og relevante»[42] for formålet med behandlingen, og § 11 e) om at opplysningene ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen. Videre kan man kanskje innfortolke et krav om å begrense innsamling av opplysninger i «nødvendighetsvilkårene» i §§ 8 og 9 ut fra synspunktet om at dersom formålet kunne vært oppnådd uten identifiserbare data så er behandlingen av opplysningene ikke nødvendig.[43] Konklusjonen må uansett være at personopplysningsloven i liten grad setter krav til eller legger føringer for minimalitet og anonymitet. Kort oppsummert oppstiller loven et forbud mot å samle inn irrelevante opplysninger og en plikt til å slette eller anonymisere opplysninger når formålet er oppnådd. Loven legger altså ingen føringer for anonymitet eller pseudonymitet i det jeg i Figur 5 har kalt «transaksjonsfasen». Det er, som vi har sett i avsnittet over, i denne fasen brukeren har en reell mulighet til å ha kontroll på egne opplysninger. Når identifiserende opplysninger først er samlet inn (videre behandling) har brukeren liten eller ingen kontroll.

I forbindelse med revisjon av personopplysningsloven er det blitt fremmet forslag om unntak fra deler av loven for personopplysninger som er «strengt pseudonymisert».[44] Forslaget er interessant i forhold til at det legges incentiver for utvikling og anvendelse av personvernøkende teknologi for å ivareta personvernet. Imidlertid er det uklart om man her tar sikte på bruk av pseudonymer i forbindelse med *transaksjoner*, eller om det er snakk om pseudonymisering av i utgangspunktet identifiserbare opplysninger (fasen «videre behandling» i Figur 5). Etter min mening er begge tilnærminger viktige, men den første varianten vil som vi har sett være klart mer personvernøkende fordi den hindrer at det samles inn direkte identifiserbare opplysninger.

40 Se f eks Schartum og Bygrave, Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger, Bergen 2004, s 93–94.

41 Se St.meld. nr 17 (2006–2007), kapittel 8.3.3 «Retten til å være anonym».

42 I direktivet er dette formulert som «relevante og ikke for omfattende». Minimalitetsprinsippet er altså noe tydeligere i direktivet, mens personopplysningsloven synes altså å vektlegge tilstrekkeliget i større grad enn minimalitet.

43 Se Bygrave, Data protection law: approaching its rationale, logic and limits, Dortrecht 2002, s 343–344.

44 Schartum og Bygrave, Utredning av behov for endringer i personopplysningsloven, 2006, radikalt forslag til ny § 3d.

Når det gjelder prinsippet om datakvalitet kommer dette imidlertid tydelig frem av personopplysningsloven, jf § 11 og formålsbestemmelsen som uttrykker at loven skal bidra til at personopplysninger blir behandlet i samsvar med «grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og *tilstrekkelig kvalitet* på personopplysninger» (min kursivering). Når § 11 stiller krav til at opplysninger skal være «tilstrekkelige og relevante» og «korrekte og oppdaterte», må dette nødvendigvis også omfatte det forhold at opplysningene som er lagret gjelder rett person. Dette forutsetter imidlertid at den behandlingsansvarlige har tilstrekkelig gode rutiner for identifisering og autentisering. Etter som stadig mer samhandling skjer elektronisk er det grunn til å spørre om ikke lovgivningen burde være tydeligere på forskjellen mellom identifisering og autentisering, jf kapittel 3.4 og 3.5. Lovens § 12 som regulerer bruk av fødselsnummer og andre entydige identifikasjonsmidler gir ikke klarhet i denne distinksjonen. Det er uklart om «entydige identifikasjonsmidler» her refererer til bruk av entydige identifikatorer og/eller bruk av autentiseringsmekanismer. En annen mulig tilnærming er å anse krav til identifisering og autentisering som et spørsmål om informasjonssikkerhet under betraktningen om at f eks utlevering av opplysninger vil være i strid med konfidensialitet eller tilgjengelighet. Dette blir imidlertid en for snever tilnærming siden spørsmålet om autentisering da først og fremst kommer på spissen i forhold til utlevering av opplysninger. Gode grunner taler derfor etter min mening for at distinksjonen klargjøres i § 11 eller i en ny revidert bestemmelse som skiller mellom adgangen til å benytte identifikatorer (f eks fødselsnummer) og hvilke krav som ellers stilles til autentisering.

5 Samlende synspunkter – veien videre

Den tradisjonelle tilnærmingen til PETs har vært minimalitet, det vil si tekniske og organisatoriske tiltak som tar sikte på å begrense adgangen til å identifisere den opplysningene gjelder. Forskningen og utviklingen innen personvernøkende identitetsforvaltning bryter ikke med PETs-tankegangen, men plasserer tradisjonelle PETs i et videre perspektiv som også omhandler sikker identifisering og autentisering.

Det er etter min mening viktig å opprettholde et skille mellom PETs og identitetsforvaltning på den ene siden og informasjonssikkerhetstiltak på den annen side. PETs og identitetsforvaltning retter fokuset på identitet og identifiserbarhet. Spørsmålet her er om det er nødvendig å samle inn identifiserende opplysninger i den enkelte transaksjon, eventuelt hvilken rolle eller identitet det er behov for å autentisere. Informasjonssikkerhetstiltak derimot tvinger oss ikke til å stille spørsmål *om* og med *hvilken identifiserbarhet* opplysninger skal

innhentes og lagres. Her er fokuset kun på å sikre de opplysninger som er blitt lagret. Begge tilnærminger er selvsagt viktige. Faren ved kun å holde fast ved informasjonssikkerhetstilnærmingen er at man ikke legger noen begrensninger på hvilken informasjon som samles inn under dekke av at informasjonssikkerheten er tilstrekkelig. Den første tilnærmingen derimot, er personvernøkende i den forstand at den gir den enkelte bedre kontroll over egne opplysninger ved at mengden elektroniske spor og lagrede identifiserbare opplysninger holdes på et minimum. Ved vurdering av hvordan tekniske og organisatoriske tiltak kan støtte opp under personvernet bør man derfor alltid starte med å vurdere spørsmål knyttet til identitet og identifiserbarhet (PETs/identitetsforvaltning), for deretter å vurdere relevante informasjonssikkerhetstiltak (f eks kryptering, tilgangskontroll etc).[45]

I fremstillingen av elektronisk kommunikasjon har siktemålet vært å synliggjøre hvordan personvernspørsmål knyttet elektroniske spor og krav til identifisering kan håndteres under synsvinkelen identitetsforvaltning. Etter min mening er det her klargjørende å skille mellom de spørsmål om identitet og identifiserbarhet som kan relateres til den grunnleggende infrastrukturen for Internett (*kommunikasjonslaget*) og de spørsmål som må finne sin løsning i form av identitetsforvaltning i *tjenestelaget*. Det siste tiåret har vi vært vitne til en voldsom aktivitet, internasjonalt og nasjonalt, knyttet til utvikling av nye standarder og systemer for identitetsforvaltning. Disse løsningene og måten de implementeres på vil utvilsomt ha betydning for personvernet ettersom Internett blir en stadig viktigere kontaktflate mot omverdenen. I den forbindelse er det relevant å se hen til den satsningen som gjøres fra norske myndigheter med å legge til rette for nasjonalt ID-kort med eID.[46] Muligheten for sikker identifisering åpner for nye e-handel- og e-forvaltningstjenester. Imidlertid er det viktig å være bevisst på i hvilke tilfeller det vil være passende å stille krav til slik identifisering. Det faktum at man har eID som sikrer sterk autentisering av identitet betyr ikke at det bør benyttes i alle tilfeller. Fra et personvernsynspunkt er det dessuten betenkelig å legge opp til en sårbar infrastrukter med kun én eID-løsning. Det bør heller legges til rette for virksom konkurranse som gir valgfrihet mellom alternative identitetstilbydere.[47] Jeg vil holde fast ved det prinsipielle som ligger i at man i alle tilfeller starter med å stille spørsmål

45 Det må antas at PETs vil kunne ha konsekvenser for informasjonssikkerhetsarbeidet ved at lagring av færre identifiserbare opplysninger medfører lavere sannsynlighet for og mindre konsekvenser av brudd på informasjonssikkerheten.

46 Justis- og politidepartementet, Nasjonalt ID-kort, Oslo, 2007.

47 Dette synes å være gjengs oppfatning i identitetsforvaltningsmarkedet, se f eks Cameron, Laws of Identity, 2007, som fremhever «Pluralism of operators and technologies» som et av syv grunnprinsipper for identitetsforvaltning.

med hvilken påstand som skal autentiseres. Er identitet overhodet relevant? Eller holder det å få etablert tilstrekkelig sikkerhet for f eks en rolle eller en egenskap? Et eksempel på denne tilnærmingen finner man f eks hos Australske myndigheter som har utarbeidet et omfattende rammeverk som skal hjelpe forvaltningen med å finne frem til hva som skal autentiseres og hvordan dette kan gjøres på en forholdsmessig og sikker måte.[48]

Det er gledelig å se at både EU og norske myndigheter uttrykker ønske om å støtte opp under personvernøkende teknologi og ser dette som en viktig strategi for å kunne ivareta personvernet (jf kapittel 1.3). Jeg mener det er all grunn til å legge videre trykk på de tiltakene som allerede er identifisert. EU kommisjonens strategi er, som nevnt, for det første å fremme *utvikling* av PETs, legge incentiver for næringslivets og offentlige myndigheters *anvendelse,* samt å heve folk flest sin *bevissthet* om PETs og personvernsspørsmål. Det er også god grunn til å følge opp Regjeringens IKT-melding som synliggjør utfordringene på dette området og som foreslår konkrete tiltak.[49] Det er ikke anledning til å diskutere disse tiltakene i detalj her. Jeg vil derfor heller rette oppmerksomheten mot en av hovedutfordringene – nemlig at PETs i liten grad har blitt tatt i bruk. Foreløpig har det vært liten etterspørsel etter PETs og få virksomheter har klart å gjøre godt personvern til et konkurransefortrinn. Grunnene til dette kan være mange, blant annet har det vært liten bevissthet blant virksomheter og forbrukere om hva som er personvernøkende og hva som ikke er det, og dermed har etterspørselen uteblitt. Den aktøren som synes best stilt til å endre denne situasjonen er det offentlige som bør ha en klar ambisjon om å legge til rette for personvernøkende løsninger. Myndighetene har f eks anledning til å stille krav til at personvernhensyn blir et førende hensyn i utviklingsprosjekter og at dokumentering av personvernøkende design (ikke bare informasjonssikkerhet) løftes frem som et kriterie i anbudskonkurranser om levering av nye løsninger. Slike krav vil gi markedsaktørene incentiver til å satse på personvernøkende teknologi, noe som vil kunne føre til økt tilgjengelighet også i privat sektor. Viktigheten av det offentliges innsats og prioriteringer på dette området kan ikke understrekes sterkt nok. Det er etter min mening naivt å tro at markedsaktørene vil satse på PETs hvis ikke det offentlige går foran som et godt eksempel.

I IKT-meldingen er regelverksendring som gir mer direkte støtte til bruk av personvernøkende teknologi et av de foreslåtte tiltakene. Jeg mener det er grunn til å holde fast ved prinsippet om teknologinøytral lovgivning. Mer

48 Se Australian Government, Australian Government e-Authentication Framework, 2005.

49 Se særlig kap 8.3.3 Retten til å vere anonym, 8.3.4 eID og valfridom og 8.3.5 Utnytting av teknologien for å styrkje personvernet.

detaljerte krav eller anbefalinger til konkrete tekniske løsninger kan med fordel utarbeides innenfor konkrete sektorer, f eks som bransjevise normer, men hører nok ikke hjemme i den sentrale lovgivningen. Et aspekt som lovgiver med fordel bør vurdere å få tydeligere frem i lovgivningen er minimalitetsprinsippet. Som nevnt i kapittel 4.2.2 stiller personopplysningsloven ikke tydelige krav til eller føringer for minimalitet (anonymitet/pseudonymitet) i transaksjoner. Ved tydeligere krav til minimalitet vil det f eks måtte dokumenteres hvorfor man har behov for å samle inn identifiserende opplysninger. Dette vil være å snu dagens situasjon på hodet hvor det selvsagte er at man behandler identifiserbare opplysninger. Et eksempel på en slik bestemmelse er å finne i Tysklands føderale personopplysningslov § 3a:

> *§ 3 Data reduction and data economy*
>
> *Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.*

Som nevnt i kapittel 4.2.2 er det videre grunn til å se nærmere på om ikke personopplysningsloven bør innføre et tydelig skille mellom adgangen til å benytte bestemte identifikatorer (f eks fødselsnummer) og krav til autentisering og bruk av bestemte typer autentiseringsmekanismer (f eks biometri).

Avslutningsvis, etter å ha pekt på tiltak som krever en betydelig innsats og oppfølgning, kan det synes som vi har en lang vei å gå i forhold til å la personvernhensyn være med på å styre teknologiutvikling og anvendelse. Det er nok dessverre også tilfellet. Samtidig er det mange og enkle tiltak som det er anledning til å gripe fatt i. Bare det å følge lovens krav om å gi god informasjon om behandlingen av personopplysninger og å gjøre den enkelte kjent med sine rettigheter vil også bidra. Til syvende og sist handler dette om å heve bevisstheten om personvernspørsmål og PETs i alle ledd i næringskjeden – fra utviklere, databehandlere og behandlingsansvarlige. Ikke minst trenger vi opplyste forbrukere og borgere som stiller krav til godt personvern.

Bibliografi

Lovgivning, forarbeider mv

Personverndirektivet, 95/46/EF av 24. oktober 1995

Direktivet om personvern og elektronisk kommunikasjon, 2002/58/EF av 12. juli 2002

Datalagringsdirektivet, 2006/24/EF, av 15. mars 2006

Lov om behandling av personopplysninger (personopplysningsloven), lov 14. april 2000 nr 31

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), lov 18. mai 2001 nr 24

Lov om elektronisk kommunikasjon (ekomloven), lov 4. juli 2003 nr 83

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), forskrift 16. februar 2004

Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret), forskrift 17. oktober 2003 nr 1246

Ot.prp. nr 49 (2005–2006) Om lov om endringer i helseregisterloven (Norsk pasientregister)

Artikkel 29-gruppen (WP 6/1997) anonymitet på Internett

Artikkel 29-gruppen (WP 68/2001) om autentiseringstjenester

St.meld. nr 17 (2006–2007) Eit informasjonssamfunn for alle

Tysklands føderale personopplysningslov, (Bundesdatenschutzgesetz), 15. november 2006

Bøker, artikler mv

Andresen, Herbjørn, «On Pseudonymous Health Registers: While they Work as Intended, they are Still Controversial in Norway», *Proceedings of the First International Conference on Health Informatics, Funchal, Madeira - Portugal*, Vol 1 (2008) 59-66

Australian Government, *Australian Government e-Authentication Framework*, (2005)

Boe, Erik, «Nye helseregistre inn bakveien?» *Kritisk juss*, Årg. 27, nr 1/2 (2000) 63-77

Brands, Stefan A., *Rethinking public key infrastructures and digital certificates: building in privacy*, (Cambridge, Mass. 2000)

Burkert, Herbert, «Privacy-enhancing technologies: typology, critique, vision», I: *Technology and privacy: the new landscape,* Agre, Philip og Rotenberg, Marc (red), (Cambridge, Mass. 1997)

Bygrave, Lee A., *Data protection law: approaching its rationale, logic and limits*, (Dortrecht 2002)

Bygrave, Lee A., «Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place», *Privacy Law & Policy Reporter*, (2002) 135-137

Cameron, Kim, *Laws of Identity*, (2007)

Chaum, David, «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», *Communications of the ACM*, vol. 24 no. 2 (1981)

Clarke, Roger, *Identity Management* (Canberra 2004)

Datatilsynet, *E-forvaltning – Datatilsynets tilrådning til regjeringen*, Datatilsynets nettsted, (2007)

EU Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)* (Brussel 2003)

European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* (Brussels 2007)

Hannemyr, Gisle, «Feil nummerbruk», *Lov&Data*, 92 (2007) 29-30

Hannemyr, Gisle, *Hva er internett*, (Oslo 2005)

Hansen, Marit et al., «Privacy-enhancing identity management», *Information Security Technical Report*, 1 (2004) 35-44

Justis- og politidepartementet, *Nasjonalt ID-kort*, Oslo, (2007)

Kent, Stephen T. og Millett, Lynette I., *Who goes there?: authentication through the lens of privacy*, (Washington, DC 2003)

L'Abée-Lund, Åsa, *Pseudonymisering av personopplysninger i sentrale helseregistre*, Oslo, (2006)

Lessig, Lawrence, *Code: version 2.0*, (New York 2006)

Mahler, Tobias og Olsen, Thomas, «Reputation Systems and Data Protection Law», I: *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies,* Cunningham, Paul og Cunningham, Miriam (red), (Amsterdam 2004)

Norsk Regnesentral, *Elektroniske spor*, (Oslo 2005)

Olsen, Thomas og Mahler, Tobias, «Identity management and data protection law: Risk, responsibility and compliance in `Circles of Trust'», *Computer Law & Security Report*, 4 & 5 (2007) 342-351 & 415-426

Olsen, Thomas og Mahler, Tobias et al, *Identity management & Privacy*, Complex, (2007)

Olsen, Thomas, «Lovgivningsprosessen bak registreringsplikt for kontantkort til mobiltelefon», *Lov & Data*, 85 (2006) 1-6

Registratiekamer, IPC og TNO-FEL, *Privacy-enhancing technologies: the path to anonymity (Vols I & II)*, (1995)

Riisnæs, Rolf, *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar*, (Bergen 2007)

Schartum, Dag Wiese og Bygrave, Lee A., *Utredning av behov for endringer i personopplysningsloven* (Oslo 2006)

Schartum, Dag Wiese og Bygrave, Lee A., *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*, (Bergen 2004)

Søiland, Arne, «Sikrere mot id-tyveri», *Computer World*, 15.01.2007, sist nedlastet 02.06.2008

Tanenbaum, Andrew S., *Computer networks*, 4th (Upper Saddle River, N.J. 2003)

Teknologirådet, *Elektroniske spor og personvern* (Oslo 2005)

Øverlier, Lasse, *Anonymity, privacy and hidden services*, (Oslo 2007)

Nettsider

Australian Government e-Authentication Framework: http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview

Credentica: http://www.credentica.com

EPAL: http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

EPIC, Privacy Tools: http://epic.org/privacy/tools.html

FIDIS: http://www.fidis.net/

GUIDE: http://istrg.som.surrey.ac.uk/projects/guide/

Jan Camenisch, IBM Zürich: http://www.zurich.ibm.com/%7Ejca/publications.html

P3P: http://www.w3.org/P3P/

Personvern på nettet, 6. november 2006, «Åpen høring om Norsk pasientregister»: http://www.personvern.uio.no/pvpn/nyheter.html

PET Workshop: http://petworkshop.org/

PICOS: http://www.picos-project.eu/

PRIME: https://www.prime-project.eu/

PRIMELIFE: http://www.primelife.eu/

TOR: http://www.torproject.org/

RATIONAL CONCERNS ABOUT BIOMETRIC TECHNOLOGY: SECURITY AND PRIVACY*

Yue Liu

1 Introduction

Across the various contexts in which it is applied, biometric technology (hereinafter also termed «biometrics») raises multiple rational concerns. This chapter aims to give some idea of the complexities involved in biometric technology by focusing on the security and privacy concerns it raises. To what extent do and will biometrics affect privacy and security? Exactly what is the special nature of biometric data compared with other personal data? Is the increasing use of biometrics just a question of «balance» or «trade-off» between privacy and security? It is with these sorts of questions that this chapter is concerned. In tackling such questions, the chapter also aims to clarify some of the misconceptions that inform parts of the legal discourse around biometrics.

2 Background

Put simply, biometric technology involves the use of automated methods for verifying or recognizing the identity of a living person based on their physiological or behavioral characteristics.[1] Most people get to know about biometrics from what they observe in science-fiction movies like Spielberg's *Minority Report*, in which people are regularly subjected to eye scans for identification, control and/or advertising purposes when they take public transport, enter office buildings, or simply walk in the street. Seductive claims have also been made about the ability of biometrics to defeat terrorism and organized crime. Biometrics figure increasingly as the centerpiece technology in implementing counterterrorist policy.

Much technology inspires not only hope but also fears. And development of innovative technology has almost always raised new legal concerns. This is certainly true in the case of biometric technology. Increasing use of biometrics

* Previously published in Computer security, privacy and politics : current issues, challenges and solutions / Ramesh Subramanian, [editor]. – Hershey PA : IRM Press, 2008.

1 See further, e.g., Wayman, J. (2000a).

has led to fears of an acceleration in the speed at which our society becomes a surveillance society with scant room for personal privacy and autonomy. Doubts have also been raised about the level of security that increased use of biometrics can actually deliver. It is further feared that the loss of privacy may lead in turn to a host of other problems, such as increasing social stigma, discrimination in employment, barriers to gaining health insurance and the like. With the growing use of biometrics, it is of paramount importance that discussions about the ethical, social, and legal implications of the technology take place. In such discussions so far, privacy and security concerns have often figured prominently[2] -- and for good reason, as this chapter highlights.

To begin with, the chapter outlines the special nature of biometric technology and biometric data. It then discusses the relationship between biometric technology and privacy. Following on from this, the relationship between biometric technology and security is analyzed in the light of technology assessment and case examples. The final section presents conclusions.

3 Special nature of biometric technology and biometric data

Generally speaking, biometric technology involves using part of the human body or behavior as mechanisms for human identification or authentication. Fingerprints, irises, faces, retinal images, veins and voice patterns are all examples of actual or potential biometric identifiers. These data are collected by sensor devices, transformed into digital representations and then, via algorithms, the data become so-called biometric templates. These biometric templates are then stored somewhere for later matching against other collected data.[3] As indicated above, the matching can be used for either authentication or identification purposes.[4] Biometric authentication involves a «one-to-one» (1:1) search whereby a live biometric sample presented by a person is compared to a stored sample previously collected from that individual, and the match confirmed.[5] This answers the question, «am I whom I claim to be?» In this process, no searching or matching a central database is necessary, although a central database can still

2 See, e.g., Cavoukian (2003); Woodward (1997a).

3 For more detailed explanation of biometric technology, see, e.g., Wayman, Jain, Maltoni, & Maio (2004).

4 «Authentication» (sometimes termed «verification») means to assess the probable truth of the claim to an identity made by a system-user; this involves a one-to-one match. «Identification» means to probabilistically link a person to an enrolled record without an identity claim. In contrast to authentication/verification, identification involves a one-to-many match. See, e.g., Wayman (2000).

5 Cavoukian, A. et al (2007) p.6

be used, provided that some other identifiable data such as a serial number is used to «look up» an individual in a biometric database, so as to find out the certain biometric template out of the database and doing a one-to –one match. Biometric identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file.[6] This also known as one to many (1: N) searches designed to determine identity based solely on biometric information. This match intends to answer the question «whom am I?» To support identification, a central database must be built containing a large set of individual biometric records. So theoretically a central database of biometric records could allow the system controller to find out who the person is provided he is already registered in the central database. During the process, the live biometric sample will be compared with all the registered biometric samples in the central database. Upon a successful match, the person's identity will be released from the central database.

3.1 The «bio» nature of biometric data and biometric technology

Compared with knowledge-based or token-based methods of authentication/identification, biometric technology is unique in the sense that it uses part of the human body or behavior as the basis of the authentication and/or identification method. What is the significance of the fact that a body-related characteristic is used as an identifier or verifier? To answer this question, we need to first investigate what biometric data are.

3.1.1 Genetic and health related data

The raw information at the heart of biometrics is by its very nature personal. It is intimately connected to the individual concerned (the «information subject»). If one takes the most popularly used and known form of biometric information – fingerprints – as an example, it has been claimed that even a fingerprint too smudged for ordinary identification could provide forensic scientists with sufficient DNA[7] to construct a «DNA fingerprint»,[8] thus providing investigators

6 Cavoukian, A. et al (2007),p.6

7 DNA (deoxyribonucleic acid) contains the genetic specifications for the biological development of all cellular forms of life. DNA is a long polymer of nucleotides and encodes the sequence of the amino acid residues in proteins using the genetic code, a triplet code of nucleotides. See, e.g., Watson (2004).

8 DNA fingerprinting is a technique by which an individual can be identified at molecular level from certain repeating sequences in the DNA present on different chromosomes. These genetic markers are known to vary from individual to individual (except in the case of identical twins). See further Center for DNA Fingerprint Diagnostics (2006), DNA fingerprinting, Retrieved June 15, 2006, from http://www.cdfd.org.in/dfpser.html.

with a powerful new tool in the search for evidence of crime. Moreover, there is a rather large body of work tracing the genetic history of population groups through the study of their fingerprint-pattern characteristics.[9] It has also been proven that there exists a mysterious linkage between certain fingerprints and certain birth defects and diseases.[10] From examining a person's retina or iris, a medical expert can determine that the person may be suffering from common afflictions like diabetes, arteriosclerosis and hypertension; further, unique diseases of the iris and the retina can also be detected.[11]

However, the informational status of the biometric templates that are generated and applied in identification/authentication systems is somewhat unclear. As indicated above, a biometric template is digitalized data of a person's physical or behavioral characteristics, not the raw information or image itself. The template is generated by application of a given algorithm. There is as yet no solid proof that the templates themselves actually contain medical information, though they are very likely to do so. A template is as unique as the raw biometric data from which it is generated. It is possible to reconstruct from a template the part of the raw biometric data that is used for creating the template.[12] Generally, templates will only contain information necessary for comparison. However, what is necessary for comparison is neither fixed nor predetermined. As the biometric template should retain the special features of the raw biometric data as identifier, it unavoidably becomes necessary to include some relatively unique and permanent features which are related to genetic information or health.[13] However, it is not certain if the information captured in the template would be sufficient for medical diagnostic purposes. Nonetheless, it is still reasonable to claim that there is generally a link between biometric information and genetic and/or health information. The latter has been widely recognized as sensitive information about individuals and, quite often, their relatives.

It has been claimed by one observer that «[b]iometrics is not a branch of medicine but rather a special form of mathematical and statistical science.»[14] The same observer goes on to state that «we should perhaps not expect to be able to determine any intrinsic meaning of biometric data, or the biometric body in general, but investigate quite specifically what uses and practices biometrics

9 See Keogh (2001) and references cited therein..
10 Woodward (1997b).
11 Cf. Bates (1991).
12 See, e.g., Jian, Ross, Uludag (2005); Bromba (2006).
13 Bromba (2006).
14 Ploeg (1999, p. 43).

will become part of.»[15] According to another observer, with almost all biometric devices, there is virtually no personal information contained therein. From my fingerprint, you can not tell my gender, you can not tell my height, my age, or my weight. There is far less personal information exposed by giving you my fingerprint than by showing you my driver's license.[16]

At first glance, these statements seem to make sense, but they are based on the assumption that technology will stop developing. It is true that there is presently no verified report about easy and fast disclosure of health information directly from biometric data; moreover, possible linkage between biometric data and health information is only reported in relation to certain kinds of biometric data. Yet as the technology develops, it is quite reasonable to predict that such disclosure and linkage may be possible in the future. The potential is clearly present. As a rule, if something can happen, it will happen. Hence, the long-term problem here is whether the data controller (i.e., the person/organization in possession of the biometric data) *will* make such linkages.

It could be countered that even if biometric data have the potential to disclose sensitive information, they are not designed to be used that way, so there is no need to worry. However, biometric features make it difficult to escape from situations of misuse in the hands of individuals or governments – with or without malicious intent. «Function creep» can occur; indeed, many privacy advocates contend that function creep is inevitable. For example, Simon Davies opines:

The history of identification systems throughout the world provides evidence of «function creep» – application to additional purposes not announced, or perhaps even intended, at the commencement of the scheme. [...] The existence of a relatively high-integrity scheme would create irresistible temptations to apply it widely, and inter-relate many hitherto separate collections of personal information.[17]

An additional purpose can be valuable or detrimental to society, but the point here is that the potential of biometric data cannot be restricted by the purposes for which they are/were originally used. There is no absolute guarantee that biometric data will not be used for revealing health information, though it would take a significant technological shift to go from current biometric systems to systems that reveal such information.[18]

15 Ploeg (1999, p. 43).
16 Wayman (1998, p. 11).
17 Davies (1994, p. 44).
18 See Feldman (2003, p. 667).

3.1.2 Relative uniqueness, universality and stability

The common idea that biometric technologies are capable of identifying individuals through one-to-many matching across large, shared databases is based on the belief that biometric identifiers are unique and universal. It has been established that each person is supposed to have unique fingerprints, irises, face and DNA. For instance, fingerprints have been used in forensic research for many years as purportedly unique identifiers of criminals. However, some recent cases have revealed that identification by use of fingerprints has been overturned on appeal at court.[19] In fact, the «uniqueness» of a fingerprint in forensic science remains an *assumption* without watertight proof.[20] The belief that latent fingerprints can be matched to a single person is «the product of probabilistic intuitions widely shared among fingerprint examiners, not of scientific research. There is no justification based on conventional science, no theoretical model, statistics, or an empirical validation process.»[21]

Nevertheless, it is worth pointing out that there is not yet any solid proof that this *assumption* is wrong either. Hence, it may be true that fingerprints *per se* are unique. Yet it does not necessarily follow that the latent fingerprint is unique too. Neither does it necessarily follow that the thumbprint template which simply extracted certain features of a raw thumbprint image can be as unique as its origin. The template may be based on a blurred, dirty and/or incomplete image of the thumbprint which may affect the accuracy of the collected biometric information, making the biometric template's uniqueness more difficult to be guaranteed. Even DNA, which is widely recognized as the most accurate biometric identifier, is exposed to criticisms. While it is true that each individual (except identical twins) has a unique sequence of genes,[22] in the forensic DNA identification process, only a subset of a particular gene is used for identification. Hence, Professor Alec Jeffreys, a pioneer in developing modern DNA testing techniques, has pointed out that DNA testing is not an infallible proof of identity:

[m]odern commercial DNA profiling compares a number of genetic markers – often 5 or 10 – to calculate a likelihood that the sample belongs to a given individual. Jeffreys estimates the probability of two individuals' DNA profiles matching in the most commonly used tests at between one in a billion or one in a trillion, «which sounds very good indeed until you start thinking about

19 See, e.g., Cole (2000).
20 See, e.g., Cole (2000).
21 Stoney (1997).
22 See, e.g., *Holladay (2002)*.

large DNA databases». In a database of 2.5 million people, a one-in-a-billion probability becomes a one-in-400 chance of at least one match.[23]

It is not guaranteed either that the fuzzy biometric template which actually uses just part of the DNA sequence will be 100 percent unique. Thus, the «uniqueness» of biometric data is not absolute, it is *relative*. The biometric templates generated from them are even less unique due to their «fuzzy» nature. This also affects the stability of the biometric data.

The universality of biometrics is also relative. One problem with the widespread use of biometrics is that there are few biometrics – apart from DNA – that everyone has. Not everyone will have a particular biometric trait, or an individual's biometric trait may be significantly different from the «normal» expected trait. For example, some people may be missing fingerprints due to skin disease – a factor which may cause more problems when enrolling a large population into a fingerprint-based register. Discrimination concerns may also be raised in such a case. Therefore, a large-scale biometric scheme will usually need to utilise more than one biometric – e.g., both fingerprint and face – to ensure that all people can be enrolled in it.

Unlike passwords or tokens, biometric identifiers are by their nature supposed to be stable over time; without such stability, their utility will be quite limited.[24] Fingerprints, irises and DNA are widely recognized as stable biometrics, while faces, keystroke and voice patterns give rise to more skepticism concerning their stability as people get older. However, the stability of even the former types of biometric data is not absolute. For instance, the image of a fingerprint pattern is «plastic» and does not remain as stable as is commonly imagined. Each time that you place your fingerprint on a finger-scanner, the pattern may appear to be the same from a short distance, but there are actually small differences in the pattern due to dryness, moisture and elasticity conditions of the skin. Moreover, cuts and scratches can alter the pattern. It is thus likened somewhat to «fuzzy» decryption.[25] Iris, another popular biometric measurement, though has been regarded as highly accurate; the process unfortunately also suffers from difficulty in consistently obtaining a valid image. The iris is often occluded by eyelids and eye lashes. In addition, data collection can also be hindered by specular reflections in uncontrolled lighting situations.[26] Similar problems also apply to other relatively stable biometric identifiers.

23 Lawless (2004).
24 See, e.g., Schneier (2000, pp. 141–145).
25 See Dorizzi (2005).
26 Retica Systems Inc. (2005).

3.2 The automatic nature of biometric data and biometric technology

Using parts of the human body as a key clue to identity is not new. It is reported, for example, that in China in the 2nd century BC, thumbprints were put on clay seals used on important documents, while in 14th century Persia, various official government papers bore fingerprint impressions.[27] Nonetheless, biometrics is presently defined as involving automated techniques. The «automated» aspect is said to differentiate biometrics from the larger field of human identification science.[28] The biometric data are processed by computers and the «bio» information is put in digital form from the moment of its creation. Compared to visual comparison of signatures or photographs, biometric identification is ostensibly less fallible and potentially much faster, and because of its «automatic» nature, biometric technology is endowed with great potential.

3.2.1 Fuzzy Unicode of individual

Biometric data have been compared with various other more traditional biocentric forms of identification such as a photograph and thumbprint that use ink print.[29] It may appear that biometric data are less[30] or at least not logically distinguishable from these images with regard to technical or moral values. But is this true?

Unlike a primitive image from which one can dissociate oneself by various superficial means, the biometric data are regarded as more reliable and accurate, though it has been recognized that there is presently no perfectly accurate biometric technology.[31] The relatively stable biometric data are associated with relatively unique biometric features. As a fuzzy match is deployed during verification or identification, the main characteristics of certain biometric features are digitalized regardless of superficial changes.

For example, the hand geometry technology uses a 32,000-pixel CCD digital camera to record the three-dimensional shape of the hand from silhouetted images projected within the scanner. The scanner does not register surface details, such as fingerprints, lines, scars, dirt, or fingernails.[32] The scanner typically takes over 90 measurements of the length, width, thickness, and surface area of the hand and four fingers. Superficial changes that may affect correct identification are thus controlled for at the outset. In this sense, the biometric data are akin to a fuzzy unicode of each individual, by which the body becomes

27 Scottish Criminal Record Office (2002).
28 Wayman, Jain, Maltoni, & Maio (2004, p. 1).
29 See, e.g., Messing v. the Bank of American 143 Md. App.1792 A.2d 312(2002)
30 See, e.g., Schneier (2000).
31 For more explanation see, Wayman, J. et al. (2004).
32 See, e.g., findBIOMETRICS.com (n.d).

an object the identity of which is determined by mathematical means. Indeed, as it has been commented, «it is possible that the expanding technologies may eventually mean that the most important identity information may be that contained in a digital body.»[33] This unicode is deemed to be relatively accurate and reliable and controlled by data controllers. Since it is a digital representation of a human being, like all other computerized data, it is easily reproduced, transmitted, analyzed and re-used while the data subjects have little if any de-facto control over it, and little if any knowledge of it or of how it will affect them in the real world. As Feldman warns: «There is a danger that the more we focus on biological characteristics, the less we remember the intangible aspects of a person's character. As a result perhaps we should be wary of moving toward a society that constantly reduces us to our biologic characteristics.»[34]

Furthermore, the fuzzy nature of the Unicode differentiates it from other existing personal code such as personal numbers or passport codes, because it is regarded as relatively stable and permanent. Certainly, while personal numbers and passport codes are unique for each person, when compromised they are technically very easy to change and they have no «physical» linkage to a certain individual.

3.2.2 Possible Linking and Tracking

John D. Woodward has pointed out that «if facial recognition or other biometric databases become interlinked, then the threat to information privacy has the potential to increase significantly».[35] Biometric identifiers provide the possibility of interlinking disparate databases in an automatic way, worldwide. This possibility depends, of course, to some extent on standardization. Currently, the interoperability of biometric identifiers is still weak,[36] but there is a trend towards increased interoperability. For instance, the International Civil Aviation Organization (ICAO) has recently adopted a global, harmonized standard for the integration of biometric identification information into passports and other machine-readable travel documents.[37] In addition, the US National Institute of Standards and Technology (NIST) has published a «Common Biometric Exchange File Format» (CBEFF) aimed at promoting

33 Harte (2004, p. 57).
34 Feldman (2003, p.666).
35 Woodward (2001a, p. 7).
36 According to the author's interview with Prof. Roger Clarke, Xamax Consultancy Pty. Ltd., Canberra, August 5, 2006.
37 The 188 Contracting States that adhere to ICAO are obligated to issue only ICAO-standard Machine-Readable Passports (MRPs) by April 1, 2010. See ICAO (2004).

interoperability of biometric-based application programs and systems developed by different vendors.[38]

Thus, the balkanization of biometric information is on its way to becoming a thing of the past and it can be reasonably expected that the linkage and tracking ability of biometrics will be developed and utilized to the full. It is not difficult to imagine a future situation in which an individual must use one particular standard biometric to pay tax, enter the workplace, go shopping, travel, obtain medical service. Such use of a biometric «key» would open up for possible linkage of each of these records and transactions, allowing in turn government or business to compile a comprehensive profile of the individual's actions.

Biometric ID systems have the potential to locate and track people physically. Of course, tracking can be accomplished without biometrics. For example, RFID, personal numbers, passwords, IP addresses can all be used as identifiers for tracking purposes. Initially, then, tracking potential seems not to be a special characteristic of biometric technology. Nevertheless, such technology does create a heightened level of concern here as it may facilitate surreptitious tracking.

Traditional authentication methods using, for example, passwords or tokens, rely on either something you know or something you have, while RFID tags usually have to be on something you wear or carry. The collection of such information requires to some extent the data subjects to *do* something, but the biometric features of individuals are not secrets, and are something you inherently have. Certain biometric features like fingerprints and facial images can be collected without the cooperation of the data subjects. However, due to its inaccuracy, particularly in large-scale matching, much current biometric technology does not have the capacity to facilitate large-scale tracking. Such tracking may be more feasible to realize sooner by using RFID technology. Nevertheless, the potential still exists for improvement of biometric technology to allow for its use in large-scale tracking in the future or to realize large-scale tracking with the help of RFID. We see an example of this mutuality in the recent development of biometrically enhanced passports that are fitted with RFID tags.

4 Privacy and biometric technology

The issue of privacy is central to concerns about biometric technology. To evaluate the various privacy concerns requires, in the first instance, an understanding

38 National Institute of Standards and Technology (2001).

of what privacy and privacy rights entail. Amongst the most influential explications of the privacy concept are the following:

- The right to be let alone;[39]
- A state of limited accessibility: secrecy, solitude and anonymity;[40]
- An interest in control of information about oneself.[41]

As the variation in these explications shows, privacy is a multi-facetted concept that is difficult to define using one simple formulation. However, this difficulty should not imply that privacy concerns lack importance. As it has been pointed out, «in one sense, all human rights are aspects of the right to privacy».[42]

Engaging in extensive debate over the exact meaning of the privacy concept is unnecessary for the purpose of this paper. It suffices to note that there are two main groups of privacy-related interests that are directly pertinent when labelling the issues that have arisen in contemporary discussion about the ethical and legal implications of biometrics. The first group of interests falls under the rubric of «informational privacy» and concerns the control of personal information. These interests give rise to attempts to establish rules governing the collection and handling of personal data.[43] Information privacy lies at the very heart of discussion over biometrics. The second interest group falls under the rubric of «physical privacy» and concerns protection from intrusive searches and seizures, particularly the protection of persons' physical selves against invasive procedures, such as drug testing and body-cavity searches.[44] The widespread use of biometric technology may invade our physical privacy in some ways, though this seems not to be regarded as the most important concern of privacy advocates. Furthermore, it is also relevant to introduce the discussion of property rights in privacy, a discussion which concerns the appropriation and ownership of interests in human personality.[45] Property notions are not necessarily inherent in privacy interests but it can be useful for the law to use the doctrine of property to protect individuals' biometric information in the private sector.

39 See Warren & Brandeis (1890–91).
40 See, e.g., Gavison (1980, p. 428).
41 See, e.g., Westin (1967).
42 Fernando (1981).
43 See Electronic Privacy Information Center & Privacy International (2005, p. ??).
44 Ibid..
45 Rothstein (1997, p. 33).

4.1 Information privacy and biometric technology

Regardless of whether an individual voluntarily provides a biometric identifier or is forced to surrender it, they are giving up information about themselves.[46] Once collected, the control over the biometric data shifts from the data subject to the organisation that has access to the data. As biometric data are intimately linked with individuals in a relatively unique way, the data are usually considered as «personal».[47] Information privacy is, therefore, the most significant concern about biometric technology. Losing control over personal data is the main challenge biometric technology poses to informational privacy, and such loss can occur in various ways.

Unnecessary collection

A central principle of rules grounded in informational privacy is that the collection of personal information should be limited to those data that are necessary and relevant to a legitimate purpose.[48] As mentioned in section 2 above, it is difficult to predict exactly what biometric technology may bring but it is clear that it has broad potential to provide an extremely convenient and cost effective way to gather and analyse biometric data. From such data, it is potentially possible to get health, racial and medical information about individuals which is not necessary for authentication or identification. This possibility also raises concerns about the possible disclosure and/or compromise of such information.

Another feature of biometric data is that they can identify people. However, when the purpose of collecting the biometric data is just for authentication, and there is little or no benefit in having stronger user identification, it is difficult to justify the collection of strong unique identifiers.

An interesting point of view concerning the health-related nature of biometric technology is that this technology benefits those who do not go to the doctor, and helps them to detect diseases earlier.[49] This claim may make sense to some extent, but the problem here is that, unless the data subjects are clearly informed about this potential and consent to it, the technology effectively makes compulsory a kind of medical check-up, thus undermining individuals' privacy interests in relation to their own health information, including their interest in being able to choose not to know certain details of health status. Moreover, the data controllers here have ordinarily no legal right to collect and keep such

46 See, e.g., Woodward (1997a).
47 See, e.g., Hert (2005).
48 See, e.g., Bygrave (2002, p. 59 et seq.).
49 Young (2001).

health information. Neither do they ordinarily have the right to share the information with other interested organizations, such as insurance companies.

Unauthorised collection

Biometric technology together with use of RFID augment the possibility of covertly collecting biometric information. Although only certain biometric patterns – e.g., facial, voice, and/or gait – can be theoretically collected without the data subject's knowledge, with help of RFID-enhanced cards, which are now being widely used for storing biometric data,[50] all kinds of personal data (including biometric data) could be collected, tracked and profiled without the data subject's knowledge or consent.

In the US legal context, the legal doctrine of «reasonable expectation of privacy» developed pursuant to the Fourth Amendment in the Constitution, has been frequently invoked in commentary on the legality of the use of facial-recognition systems and other biometric technologies in public spaces. Here, our primary focus will be on facial-recognition technology which is widely used for covert collection of biometric information. It has been argued that people have a reduced expectation of privacy in public settings, and, additionally, that no individual can reasonably expect to maintain privacy in a public forum.[51] Based on a discussion of the US Supreme Court decisions in *Katz*[52] and *Kyllo*[53], McCoy has listed several reasons why facial recognition does not violate privacy:[54]

1. Facial recognition is implemented in an open field; there cannot be a reasonable expectation of privacy in public places.[55]
2. Video surveillance is not a search regulated by the Fourth Amendment because it is capturing exactly what the naked eye beholds. «What a person knowingly exposes to the public…is not a subject of fourth Amendment protection.»[56]
3. Facial-recognition technology only identifies criminals who are filed in the system's databases and does not automatically store images of ordinary citizens who pass by its line of sight. Biometric technology was designed to locate and identify criminal not innocent people.

50 See further Cavoukian (2004).
51 See, e.g., McCoy (2002) and references cited therein.
52 United States v. Katz, 389 U.S. 347 (1967).
53 Kyllo v. United States, 533 U.S. 27, 33 (2001).
54 McCoy (2002).
55 See Kyllo, 533 U.S. 27, 33 (2001).
56 See Katz, 389 U.S. 347, 351.

4. Facial-recognition technology does not violate privacy rights because it is merely making a procedure currently used by law enforcement more efficient; it employs the same procedures as fingerprinting. If fingerprinting does not violate the constitution, then neither should facial-recognition technology.

These arguments are very interesting. At the same time, they expose much misunderstanding of the biometric technology concerned as well as a controversial understanding of the legal doctrine of «reasonable expectation of privacy». There is no simple answer as to whether facial recognition violates the right to privacy, as it can be applied in various ways some of which are more privacy friendly (or privacy invasive) than others. However, it is generally the case that a covert facial-recognition system is inherently privacy invasive.

Certainly, it is true that people generally have less reasonable expectation to privacy in public places. Yet it is also emphasised that notions of privacy remain tied to the individual rather than certain categories of space.[57] Although the Court in the *Kyllo* decision invalidated the disputed search because it occurred in and around a residential home, it does not follow that there is no privacy or reasonable expectation of privacy in existence at other places; it only means that the protection of privacy in respect of those other places may be more controversial or difficult to uphold. Whether the use of facial-recognition systems or other biometric technology in public places violates privacy depends on specific applications.

McCoy compares facial recognition with video surveillance in general, claiming that face is something that one «knowingly exposes to public». This argument is based on a misunderstanding of the biometric technology. Biometric facial-recognition systems are not the same as general video surveillance. Video surveillance is just a simple recording of what happens in the public sphere, while facial recognition systems target the detailed facial images of individuals, collect these images and generate biometric templates for subsequent matching against other saved biometric templates in a database. Theoretically, the matching can be both one-to-one and one-to-many.[58] Generally, unless a special privacy-friendly system is applied, the templates stored in the database are also linked with other personal information. Once a positive match is found, a determination of identity is made. In the facial-recognition scheme, people are

57 Kyllo v. United States, 533 U.S: 27, 33 (2001). at 32–33

58 The facial recognition technology in practice has very high false acceptance and false rejection rate, and at present it is not yet accurate enough to undertaken large scale matching task, especially identification. One to many match is even less likely to happen in such large scale settings as airport or subway, due to the present technology limitations.

checked against a database one by one; they are, as a point of departure, all under suspicion, and for no apparent reason.

In video surveillance, people are typically only subjected to attention and identification when they actually commit some crime (or carry out other non-conformist actions), and law enforcement officials usually need to go through the recordings made at certain time in a certain place before they can find their targets. Criminals will generally not attract special attention under such systems if they do not do something overtly illegal. For example, video surveillance of a shop will usually not pick out a person unless they steal goods; otherwise they remain anonymous and are not checked against some database. Whether this kind of surveillance is problematic is outside the scope of this paper, but it is clear that the biometric facial-recognition system is more privacy invasive than ordinary video surveillance.

In the public place, it is true that a person's face is not a mystery to the world, yet it is arguably true also that facial-recognition technology enables access to considerably more information than would be available to the ordinary public view of a police officer; the technology reveals, in other words, more than just a face. And, generally, the data subjects will effectively have no right to refuse such scanning. Even if an individual expects to be watched by law enforcement officers, they do not generally expect to be automatically checked against a particular database and then monitored if a positive match is made. But this is what happens with facial-recognition systems: «To the extent that the database tracks the location of faces it successfully scans, it operates as a homing device on a person's movements.»[59]

It may be argued that only an individual whose templates happen to match the saved data on a criminal is recorded and monitored. However, this is also another naïve misconception of the biometric technology. Facial recognition can be used both for authentication and identification, depending on the kind of application adopted. There are various ways the facial recognition system can be applied. For verification purposes, all individuals' facial images are collected. This is the case, for instance with the US VISIT program: visitors' facial images are collected in advance, and saved in a huge database with their other personal data. The facial recognition can be used in various ways, and the level of privacy invasiveness depends on how it is applied. There is no absolute guarantee that innocent people's biometric templates will not be stored, or matched for verifying their identity and tracking their movements.

It is claimed above that facial recognition is «merely making a procedure currently used by law enforcement more efficient» and the comparison is

59 Brogan (2002).

drawn to fingerprint matching in forensic science and the police officer standing in a crowd with a stack of mug shots, comparing them to people who walk past him. This is again another misconception of facial-recognition technology. In the traditional manual settings described above, whether this be fingerprint matching in the laboratory or police detection by the roadside, there is a certain time, certain place, certain purpose and certain reason for the checking process. The policeman stands at a certain place checking people pass by because it is a place where a certain criminal or criminals may appear, and it is only these persons who are the aim of the surveillance. The latent fingerprint is matched against the database of criminals because it is collected at a crime scene. However, in the case of biometric matching, the surveillance is different. The facial-recognition system is operated at various places, various time, and for no specific purposes. Generally, the installation of a facial-recognition system aims not to find one or several particular criminals out of thousands of people passing by. Such an aim is in fact very difficult to achieve for such large scale matching, due to current technological limitations. As it has been commented, «[t]he area where the technology has not yet matured is in the area of surveillance. Contrary to the portrayal of face recognition technology and popular culture, the technology cannot easily pick a face out of a crowd».[60] (Its ability to do so in the future, however, will make for an even more privacy-invasive society.) More likely, the system will scan the images for verification purpose or store them for later matching. It is actually more like a general mass surveillance, but with more invasive measures. Most important of all, individual's personal data are collected for no particular reason.

Unauthorised use: function creep

The unauthorised use of biometric data is the greatest risk that biometric technology poses to informational privacy. Unlike other personal data, biometric data are special by their nature, which also determines the great potential of their various uses. It is not the intended use of biometric technology that is seen as problematic, but the other possible purposes it may be used for.

For example, fingerprints have been used in forensic identification. The collection of such information will facilitate police searches. By virtue of this, the database of biometric information could be used as a database of criminal records. Law enforcement authorities will be able to conduct surveillance on the general population without any evidence of wrongdoing.

Moreover, as a relatively unique identifier, biometric data not only enables individuals to be tracked, but creates the potential for the collection of

60 Kenyon (n.d.).

individual's information into a comprehensive profile by linking the various databases together. The automatic nature of biometric identifiers makes it easy to copy and otherwise be shared among countless public and private sector databases. An article in a hotel trade publication points out that «with the use of this (biometric) technology a front desk clerk could know instantly at check-in that Mr. John Smith during his last stay purchases: three Cokes from the minibar, two martini's in the lounge, ate dinner at the hotel restaurant where he ordered the special and since his last visit has moved from Chicago to Atlanta».[61] The record of Mr Smith's alcohol consumption may be used by his insurance company who may be curious about Mr Smith's alcohol consumption and want to rank his risk of getting a heart or liver disease. Information in this profile may be used out of context to the detriment of the data subject, and unjust decisions about them would be made simply by automatically analysing this profile, which may contain incomplete or inaccurate data. And all this could be done without the consent or knowledge of the data subjects.

As indicated above, «function creep» is unavoidable.[62] The widely-cited example on point is the US Social Security Number, which is used for a broad range of purposes.[63] It has been claimed that «any high-integrity identifier (like biometrics) represents a threat to civil liberties, because it represents the basis of a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behaviour would become transparent to the state, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists.»[64]

Loss of Anonymity

Anonymity has been frequently linked with autonomy; it is a key to people's sense of freedom. The ever-increasing quantity of personal data online makes it more and more convenient to track and profile individuals by government or private organizations. Consequently, anonymity may turn out to be the only tool available for ordinary people to defend themselves against being profiled. However, widespread use of biometric technology will substantially undermine people's ability to be anonymous. It has been argued, though, that it is possible to use biometric technology for anonymous authentication.[65] Yet it has also been pointed out that if one really wants to be anonymous then biometric technology is not the appropriate technology of choice since biometrics, by nature,

61 Rinehart (2001).
62 Davies (1994).
63 See further Woodward (1997, p. 1486) and references cited therein.
64 Clarke (1994, p. 34).
65 Grijpink (2004). See also Impagliazzo & More (2002).

are generally inconsistent with anonymity.[66] Biometric systems are created to identify or authenticate people, and it will generally not be a large task to link, directly or indirectly, a biometric identifier to other personal data.

Woodward has argued that «to the extent there is less individual anonymity today than in decades or centuries past, biometrics is not to blame.»[67] He goes on to claim that while a biometric identifier is very accurate, «it is not the first nor is it the only identifier used to match or locate information about a person.»[68] Therefore, he concludes, «it is not obvious that more anonymity will be lost when biometrics is used.»[69] These arguments seem to make sense at first sight, as they use a fact as their premise, yet the conclusion drawn is misleading for the following two reasons:

First, the author underestimates the reach of biometric data. He uses «name», «social security numbers» «account numbers» as examples of «other numerical identifiers» to compare with biometric data, and infers that since there were many other identifiers before biometrics, the latter should not be blamed for lack of anonymity. As discussed before, biometric data are special by their nature and by their usage potential. There is no existing identifier such as name or social security number that can be really equate with biometrics. Names can be changed, misspelled and numerous same names in the world can be found. A social security number is not universal at all; it is often restricted to a particular jurisdiction. As for account numbers, it is not usual to see people use these as authentication methods other than for obtaining financial service, and such numbers can also be changed and/or restricted to a certain location and time period. As a matter of fact, no existing identifier can expose so much about us as biometric data can, nor is there any other identifier that is *supposed to be* so universal, long-lasting,[70] and intimately linked to us as biometrics. To say that the use of biometrics will not cause more loss of anonymity is overly optimistic.

Second, Woodward infers that because biometrics are not the only identifiers that may erode anonymity, biometrics should not be blamed for such erosion. This is like saying that because A is not the only person that commits this crime, he should not be punished or stopped. Despite the fact that there exist

66 Personal interview by author with Dr. Ted Dunstone, Chair of the Biometrics Institute in Australia, Sydney, August 14, 2006. See also Crompton (2002).

67 Woodward (2001).

68 Woodward (2001).

69 Woodward (2001).

70 Due to the limitation of the biometric technology, no biometric today provides lasting signatures on electronic transactions, though it is supposed to be. We will return to this in section 4 about security and biometrics.

many means to erode anonymity in the modern world, it still cannot be denied that biometric systems are detrimental to anonymity.

4.2 Physical privacy and biometric technology

Physical privacy is the right to be free from unwanted, unreasonable intrusions or searches into one's body. It is concerned with bodily integrity (and, indirectly, emotional integrity, together with human dignity). Issues revolving around physical privacy include schemes for compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation.[71] Physical privacy is also defined as freedom from contact or monitoring by others.[72] In the biometric context, the question is whether the collection of biometric data amounts to an intrusion into a person's body. Most capture of biometric data requires some infringement of the data subject's personal space. Iris and fingerprint scanning require close proximity of biometric sensors to the body part. The adoption of other types of biometric technology may incur use of relatively invasive processes, such as substance-abuse testing, body screening and genetic screening, and may therefore be regarded as intruding into persons' physical privacy, even if the collection of biometric data is unsuccessful for various reasons. It is noteworthy that in the US legal context, «searches» under the Fourth Amendment of the US Constitution may include the gathering of physiological information from individuals.[73]

In the discussions on the relation between biometrics and privacy, moral and legal concerns about physical privacy usually take a backseat to concerns about informational privacy. The reason for this is clear: the «physical intrusion» of biometric technology usually combines with the collection of physical information. The mere fact that an individual is subject to «intrusion» by biometric technology is not the focus of most legal and social commentators, because the harm of this «physical intrusion» is not regarded as strong as the consequence of losing control of one's biometric information.[74] Yet for some people with certain cultural or religious backgrounds, the mental harm of this physical intrusion may be quite serious.[75]

71 Clarke (2000).
72 See, e.g., Griswold v. Connecticut, 381 U.S. 479, 494 (1965).
73 Smith v. U.S., 324 F.2d 879 (1964).
74 To the author's knowledge, there are no documented cases of biometrics actually causing direct physical harm to a person.
75 See, e.g., Woodward (1997, p. 1488) and references cited therein.

Some authors consider as an invasion of physical privacy the possible harm to hygiene which could be caused by biometric technologies and the use of biometric sensors.[76] However, this view stretches the notion of privacy too far. Biometric technology may infringe an individual's right to full health, but hygienic problems do not directly violate the right to privacy as such. Biometric technology may cause violation to physical privacy when it consists of unreasonably intrusive collection of biometric data, even if no actual physical harm is suffered by the data subject.

4.3 Property rights?

Thomson has argued that the right to privacy interacts with the justification of property rights.[77] Although I agree with Scanlon, Inness[78] and many other authors that the right to privacy is not based on a property right, it may be beneficial to create a property right in relation to commercial exploitation of our biometric data. Being intimately linked to an individual and helping to make them special and unique, such data ought arguably to belong to the individual from whom they are ultimately derived. Recognition of a property right over our personal information may enhance the protection of our privacy right, especially in the commercial world. As Flaherty has pointed out: «Although I have a congenital dislike for the notion that one should be allowed to sell one's privacy to the highest bidder, almost everything else is for sale in our capitalistic societies. In this case, in fact, we have been giving away our personal, private information for free, because we are not smart enough to insist on payments for its use at the outset.»[79]

The discourse of property rights, particularly during the nineteenth century, has been a liberal discourse focusing on individual freedoms and rights. The category of «property» has marked the boundary of the public /private dichotomy.[80] There have also been suggestions that genetic information should be shared as a form of «familial» property amongst family members who have

76 See further Woodward (2001b).
77 Thomson, J.J. (1975), pp.295–314
78 See, Inness, J.C. (1992), pp.28–39; Scanlon, T. (1975), pp.315–322
79 Flaherty, D.H. (1999), pp.19–38, Edited by Bennett, C. and Grant, R. Toronto, Buffalo London: University Of Toronto Press. A good example is the www.findpeople.com, in which you can find any person in the USA that has a record. You can get a full record of the person's history, age, telephone number criminal record etc. by paying certain amount of money, and the company will keep you confidential from the data subjects, which means the company actually make benefit out of people's personal information without their knowledge about it.
80 Vandervelde, K. (1980).

a legitimate common interest in the information.[81] An important catalyst for debate over the proprietary aspects of body-related information was the decision of the Californian Supreme Court in *Moore*.[82] The court refrained from extending property rights to individuals over their own body parts, stating that to do so would have too broad of a social impact and that such an extension must be carried out by legislation. At the same time, the court seemingly felt at ease when affirming the defendant's property rights over the cell line derived from Moore's tissues, asserting that this cell line was manufacture created from the labour of the researchers.

The court's decision is highly controversial and attracted much criticism. US legislation has gone on to adopt an apparently different approach, on the basis that Moore's case «fails to adequately protect a patient-donor's individual liberties and further fails to provide patients with any incentive to allow research utilising their tissue».[83] The US Federal Genetic Privacy and Non-Discrimination Act (1995) grants (in section 104(a)) a federal property interest in an individual's own genetic material, including DNA and tissue samples.[84] Moreover, New Jersey legislation has gone a step further to provide a private property right in a person's genetic information. Both pieces of legislation establish a cause of action to enable aggrieved individuals to seek civil remedies against an offender that attempts to violate these property rights.[85]

In the biometric context, the property right in privacy is frequently raised in connection with the biometric data stored in databases or smart cards. Whether biometric data per se or certain kinds of biometric data should be regarded as genetic information or genetically-related information is still debatable. Nevertheless, the introduction of a property right in privacy can at least provide an effective means of privacy protection when biometric data are concerned. The right to property in privacy is based on a moral value of privacy, but it also entails the legal power to possess, use, transmit, exchange or alienate objects. Because the property right is a negative right, which requires other people to refrain from interfering with an owner's possessing, using and handling the things that are owned, without the owner's consent, it can create a solid legal basis for the data subject to restrict others from infringing their control over their biometric data. If unauthorised use of biometric data occurred, data subjects would have arguably have a stronger legal basis for requiring increased damages payment. The right would not stop data controllers from

81 Wersz D Cet al (eds.). (1995).
82 Moore v Regents of the University of California, 51 Cal.3d 120(1990).
83 Lin (1996).
84 Charatan (1996).
85 Lin (1996, p. 129).

collecting or reusing biometric data, but will compel them to pay royalties to data subjects for making commercial or non commercial use of them.

5 Security and Biometric technology

Biometric technology has been frequently linked with security goals. For example, it is extolled as the most secure and convenient form of authentication because biometrics «cannot be borrowed, stolen, forgotten or forged.»[86] There has also been discussion about the balance between security and privacy, including biometrics' inroads on civil liberties in the name of public safety. Yet, as pointed out by Clement, the so-called «trading off» between privacy and security is an inappropriate way of looking at the issue – «a distraction that prematurely concedes and obscures a dangerous presumption.»[87] The strong conviction in the efficacy of technology may really be a romanticized illusion. Human beings have an almost blind faith in all things scientific,[88] and biometrics are certainly cloaked in a «scientific» mantle.

5.1 Technology limitations

No biometric technique is completely accurate. Facial recognition, the primary biometric selected by ICAO in 2002, has actually a very low accuracy percentage in uncontrolled lighting situations, and the false positive rate (FPR) is unknown in large-scale applications.[89] In the real world, to accurately identify suspects under uncontrolled situations out of a large group will arguably be very difficult, and the system will also be affected by such things as age and glasses. Even iris recognition, which has been widely accepted as based on a relatively very accurate biometric, is still not sufficiently accurate for common deployment.[90] Most biometric technology has not yet been proved to be successful under large-scale applications. A report released by the European Commission in March 2005 warned that, on the technological side, there is currently a lack of independent empirical data.[91] Bruce Schneier, a specialist on security issues, observes that even with a 99.9 percent accuracy rate, the result would be frequent false positives, perhaps in the number of hundreds or thousands, at sites where there were large numbers of individuals, such as

86 See Subcomm, H.R. (2001, p. 42).
87 Clement et. al. (2002, p.195).
88 See further Wayman (2000b).
89 See, e.g., Ezovski (2005).
90 See further Gomm (2005, October 21).
91 European Commission's Joint Research Centre (2006).

at airports. In the end, guards would come to disregard all hits, rendering the system useless.[92] However, it has been argued that biometric technology can at least be more accurate than human beings in checking identity.[93] Unfortunately, no solid evidence has yet been established to prove this claim. Even if it is true, it does not necessarily follow that biometric technology can perform its task satisfactorily in light of the considerable money and effort it costs, nor that it can be an adequate substitute for traditional authentication methods. As Dr. Ted Dunstone has emphasised, it is just an alternative and a convenient one.[94]

Professor Andela Sasse, a biometrics expert, recently advised UK parliamentarians that biometric technologies were «a lot less mature» than manufacturers made out.[95] Biometric technology is based on the assumption that human pattern recognition, finger prints, irises and faces will stay the same over time, which is not true. Moreover, «even if the underlying biological traits of interest are truly unique, it does not follow that our machinery will be able to measure them faithfully.»[96] The *relatively* unique and stable nature of biometric data causes a lot of technical problems for the accuracy of biometric technology.

There are other practical problems with biometric technology too. In Germany, where the e-passport scheme has been started, complaints have arisen about various aspects from price to privacy concerns, as well as technique difficulties. Teeth and smiles can confuse the facial recognition system, and the distance between the chin and forehead on the photo must be not less than 32 mm but not more than 36mm. It is not easy for people to abide by all these specifications.[97] Furthermore, there can be at least the perception of discrimination against certain group of people who are unable to use the biometric system for reasons of ethnicity, physical disability, medical conditions etc.

Biometric technology has been long recognized as a useful weapon to combat fraud. However, the computer systems that are used to process biometrics are exposed to the same kind of manipulation as other computers. People can access, erase, or alter what is stored there. «In the end, security depends upon people…but the weak link is the systems, procedures, and people who implement them.»[98] In addition, there are reports of cases in which the system

92 See Schneier (2003, p. 189).
93 Interview by author with Dr. Ted Dunstone, Chair of the Biometrics Institute in Australia, Sydney, August 14, 2006.
94 Interview with Dr. Ted Dunstone, Chair of the Biometric Institute in Australia, Sydney, August 14, 2006.
95 US Fed News Service (2006).
96 Wilson (2005, p. 4).
97 Laitner & Williamson (2005, p. 8).
98 Norman (2003).

can be fooled without difficulties. For instance, studies have shown that thin fingerprint-pads adhered to fingers have managed to fool scanners.[99] Just recently, a German computer security consultant has shown that he can clone the electronic passports that the United States and other countries are beginning to distribute.[100] More sophisticated methods of biometrics fraud may also appear with the development of technologies. It goes without saying that to steal or reproduce a fingerprint is still more difficult than stealing a key or a smart card, but we have to be clear that it is not always necessary to steal the real finger or iris to compromise the system.

5.2 Misconceptions of biometric technology

The technology limitation of biometric technology is, however, not a complete indictment of the technology. The more serious problem is the misconception about the security level that biometric technology can guarantee for us.

The difficulty of challenging a false biometric match is particular troubling in situations that involve government agencies or criminal investigations. For example, over-reliance on digital images of fingerprints led the FBI to wrongly suspect an Oregon lawyer of involvement in the 2004 Madrid train bombings.[101] In that case, the suspect was lucky enough to be released when the Spanish investigators matched the fingerprints to an Algerian, forcing the FBI to admit it was wrong. However, in cases where no other match is found, and there exist a false match and an overconfidence in the technology, innocent people could remain in jail.

Another extreme is that «the reliance on such flawed security measures might ultimately compromise security further by reducing vigilance and paying less heed to other warning signs.»[102] The Ressam case reflects that it was purely human skill that prevented a terrorist attack.[103] When Ressam attempted to enter the USA, he had an authentic Canadian passport issued under a false identity. The computer system cleared him by his ID, but custom agents felt he was suspicious because he was sweating, fidgety and avoided eye contact. Hence, the most relevant question we need to point out here is that the ability to accurately identify an individual does not mean that we really know what the individual would do, unless he is already in our suspect list, and we identify him from the database. As for numerous potential terrorists with clean

99 See Higgins (2003).
100 See Zetter (2006).
101 Leyden. (2004).
102 Roy (2005).
103 See further Schneier (2000, p. 58).

backgrounds and authentic ID, biometric identification can do nothing. The ability of finding out «who you are» does not mean that we necessarily know what an individual had committed and what he might commit. It has been shown that even with biometric technology at hand, the terrorists behind the 9/11 attacks would not have been stopped.[104]

5.3 Security problems posed by biometric technology

As we can see from above discussions, biometric technology is far from mature as it is portrayed to be. In practice, it will inevitably commit various errors. These errors are likely to be compounded by the frequent absence of «fall-backs» in the event of identity theft.[105] No security system is perfect, and a truly secure system always contains a well-functioning fall-back measure when critical breach happens. Generally, once a biometric is compromised, it is compromised forever. In the event of biometric identity theft, there would appear to be no alternative but to withdraw the user from the system.

It has been reported, though, that some research has shown it is possible to transform a biometric iris template so that it assumes a new format that is unique to a particular application. Thus, a template generated in a format corresponding to a particular application A could not be misappropriated and used to authenticate a user for application B.[106] In addition, there is also reports about research on cancellable biometrics.[107] Instead of enrolling with your true finger (or other biometric), the fingerprint is intentionally distorted in a repeatable manner and this new print is used. If, for some reason, your original fingerprint is stolen, an essentially «new» fingerprint can be issued by simply changing the parameters of the distortion process. This technology may enhance the security level of biometric technology, but several problems still remain:

- It might not protect against replay attack, if the attacker has copied the user's actual biometric character (by, e.g., photographing the iris).[108]
- In the first method of using different formats in extracting the iris template, it may mean some information is thrown away. If each template from the one character is different, then each template has fewer bits of entropy that it would have if it were only one. That is, each template is

104 Turley. (2000).
105 Wilson. (2005, p. 18).
106 See further Braithwaite, Seelen, Cambier, Daugman, Glass, Moore, & Scott (2002).
107 See further Cowley (2005).
108 E-mail correspondence from Mr. Stephen Wilson, Chairman of Lockstep Consulting (www.lockstep.com.au), September 7, 2006, on file with author.

«fuzzy» and this has to erode the accuracy, leading to higher false match rates.[109] Generally accuracy and whole image are required for biometric identification.[110]

- These methods are still very much at experimental level, and are not ready for commercial deployment for the next several years.[111]
- It is not known for sure how much correlation there is between one template and another. If an attacker can get hold of a template (and/or the original biometric character) they may be able to predict what the next generated template will look like.[112]

Besides these problems, it is clear from many existing biometric applications and biometrics advocates that building up a centralised personal database with links to identification and verification systems is supposed to be a fundamental part of the whole biometric system. This also creates a great «honey net» for crackers. The implementation of a centralised system would require widespread access from various remote locations. This may generate significant numbers of failures and make the system prone to be cracked by «physically accessing one of the sites, by finding some communication-based vulnerability, or by bribing or corrupting someone with access to the system.»[113] Through this access, identity theft or alteration of data could be achieved without many difficulties. Moreover, with such a complex centralised «security» system, a failure at one location is likely to cause cascading effects throughout the whole system. Such kinds of failures can be achieved either through a physical attack on the infrastructure or a cyber-attack.[114] It has been noted that especially in the absence of costly dedicated networks, an Internet-based system would «inevitably be the target of malicious attacks as well as subject to unintentional or incidental damage».[115] In other words, the so-called «security» system would actually generate less security and more vulnerability.

Will it then be more secure to store the biometric templates in a portable device? It has been argued that the best method to avoid central storage and to be both secure and privacy friendly, is to store the biometric information on

109 Id.
110 E-mail correspondence from Prof. Roger Clarke, Xamax Consultancy Pty. Ltd., Canberra, September 7, 2006, on file with author.
111 E-mail correspondence from Mr. Stephen Wilson, September 7, 2006; E-mail correspondence from Dr. Ted Dunstone, September 8, 2006, on file with author.
112 E-mail correspondence from Mr. Stephen Wilson, September 7, 2006.
113 See Kent (2006).
114 Id.
115 Id.

a portable device, such as a mouse, mobile, laptop computer, or smart card. However, this solution has been criticized as «a worrying gimmick, closely equivalent to writing the PIN on the back of your credit card.»[116] A majority of commercial fingerprint detectors can be fooled by replica prints. So if you lose your phone or smart card a clever thief will find your biometric security information very conveniently left behind all over the keypad.[117] A robust liveness detection system is needed to combat such fraud, yet in commercial practice, it remains uncommon in fingerprinting systems.[118]

Another major security concern is that biometric technology adds a new dimension to identity theft.[119] For instance, when a national ID card with biometric identifier is used, the weaknesses of a card system may increase the risk of identity theft. Criminals and others could masquerade as someone else at the point when the card is issued – this could become a very effective form of identity theft.[120] A widely used biometric identifier at various occasions may actually facilitate easier identity theft at one place. Once this happens, it will be extremely difficult to issue another biometric identifier or prove it actually happens. Although some people argue that biometric technology will be a good solution for combating identity theft, biometric identifiers will not solve the problem of identity theft facing the elderly community. Biometric systems in use now are successful because the number of people enrolled is limited. When the system fails, human administrators are available to assist in the authentication process. Creating an automated system on a national scale is beyond the capability of any of the existing technologies. Simply by merging the existing systems into a single central database would cause the reliability of those systems to be lost. Further, biometric databases would be subject to new forms of abuse which may be more difficult to correct and will pose significant consequences for individuals whose biometric identifier is compromised.[121]

6 Future trends and Conclusions

It is impossible to turn back the tide of biometric technology. The emergence of this technology is a prominent landmark not just in the parochial technology perspective. It may be premature to compare the arrival of biometric technology with the opening of the Pandora box, but the impact could be similarly

116 Wilson, S. and Prints, T. (2004).
117 Id.
118 Wilson (2005, p. 12–20).
119 Clarke (2001).
120 Neill (2005).
121 Rotenberg (2002).

far reaching. In common with the challenges of facing any new technology, biometric technology must be approached from multiple perspectives and a broader understanding of the issues in the wider context, weighing the various rationales, practical technological realities and limitations.

As biometric technology advances, its current state of effectiveness still leaves much to be desired. The inherent nature of biometric technology provides enormous potential for undermining privacy, despite the fact that, as it stands now, such technology does not offer all the matching, tracking and linking possibilities that are commonly envisaged. The inaccuracies and the security risks posed by biometric technology have, rather ironically, added more security problems, something not generally known. As mentioned previously, biometric technology for the near future at least is more likely to function as a convenient alternative or supplement to traditional authentication methods than as a security enhancement tool.

The key issue regarding biometric technology is not choosing between security and privacy. If we allow ourselves to see through tunnel vision and balance solely the enhancement of security against the sacrifice of privacy, then the trade-offs are easily cast in doubts. The present developing biometric technology does not actually offer the gains in security as expected, in spite of the invasion of privacy that occurs when it is implemented. If biometric technology is going to be adopted without strict restrictions, then it casts into doubt the very value of liberty and privacy it is designed to protect. Even if the creation of a surveillance society may insulate us to some extent from some types of security threats, it may very well swap one inequality for another, and in the process, raise more problems than it solves.

Nonetheless, it is also true that a lot depends on the details surrounding the various biometric technologies and their related applications. Biometric technology may evolve to be more privacy friendly and security enhancing than it is now. It is important to recognise that privacy and security are not necessarily two contradictory concepts where biometrics is concerned. The means and application of biometric technology are the key issues here. They need to be further studied by technical experts as well as law and policy makers.

References

Bates, B. (1991). *A guide to physical examination and history taking* (5th ed.). Hagerstown: Lippincott Williams & Wilkins.

Berman, J. & Mulligan, D. (1999). Privacy in the digital age. *Nova Law Review, 23*(2), 551–582.

Braithwaite, M., Seelen, U. C. V., Cambier, J., Daugman, J., Glass, R., Moore, R., & Scott, I.(2002). Application-specific biometric templates , IEEE Workshop on Automatic Identification Advanced Technologies, Tarrytown, NY, March 14–15. Retrieved February 1, 2007, from www.cis.upenn.edu/~cahn/publications/autoid02.pdf

Brogan, J. D. (2002). Facing the music: The dubious constitutionality of facial recognition technology. *Hasting Communications & Entertainment Law Journal, 25*, 65–81.

Bromba, M. (2006). On the reconstruction of biometric raw data from template data. Retrieved February 1, 2007, from http://www.bromba.com/knowhow/temppriv.htm

Bygrave, L. A. (2002). *Data protection law: Approaching its rationale, logic and limits*. The Hague: Kluwer Law International.

Castle, M. N. (1998). *Hearing on biometrics and the future of money*, Committee on Banking and Financial Services, Washington, D.C., May 20.

Cavoukian, A. (2003). *National security in a post 9/11 world: The rise of surveillance…the Demise of Privacy?* Retrieved February 1, 2007, from http://www.ipc.on.ca/images/Resources/up-nat_sec.pdf

Cavoukian, A. (2004). Tag, you're it: privacy implications of radio frequency identification (RFID) technology. Retrieved February 1, 2007, from http://www.ipc.on.ca/images/Resources/up-rfid.pdf

Center for DNA Fingerprint Diagnostics. (2006). DNA fingerprinting. Retrieved February 1, 2007, from http://www.cdfd.org.in/dfpser.html

Charatan, F. B. (1996). New Jersey passes genetic privacy Bill. *British Medical Journal, 313*, 71.

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People, 7*(4), 6–37.

Clarke, R. (2000). Beyond the OECD guidelines: Privacy protection for the 21st century. Retrieved February 1, 2007, from http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#Priv

Clarke, R. (2001). Biometrics and privacy. Retrieved September 6, 2006, from http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

Clement A., Guerra, R., Johnson, J., & Walder, F. (2002). National identification schemes (NIDS): A remedy against terrorist attack? In K. Brunnstein & J. Berleus (Eds.), *Proceedings of the sixth conference on human choice and computers: Issues of choice and quality of life in the information society* (pp. 195–205). Boston: Kluwer.

Cole, S. (2000). Myth of fingerprints: A forensic science stands trial. *Lingua Franca, 10*(8), 54–62.

Cowley, S. (2005). IBM works toward replaceable biometrics. Retrieved September 5, 2006 from http://www.csoonline.com.au/index.php/id;260154133;fp;8;fpid;8

Davies, S. (1994). Touching big brother: How biometric technology will fuse flesh and machine. *Information Technology & People, 7*(4), 38–47.

Dorizzi, B. (2005). Biometrics at the frontiers: Assessing the impact on society. Technical impact of biometrics. **B**ackground paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission. Retrieved February 1, 2007, from http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/TechnologicalImplications_Dorizzi.pdf

Electronic Privacy Information Center (EPIC) & Privacy International (PI). (2005). *Privacy and human rights: An international survey of privacy laws and developments*. Washington, D.C.: EPIC/PI.

European Commission's Joint Research Centre (JRC) (2006). Biometrics at the Frontiers: Assessing the Impact on Society. Retrieved February 1, 2007, from ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf

Ezovski, G. M. (2005). Biometric passports: Policy for international and domestic deployment. *Journal of Engineering and Public Policy, 9*. Retrieved February 1, 2007, from http://www.wise-intern.org/journal/2005/Ezovski.pdf

Feldman, R. (2003). Considerations on the emerging implementation of biometric technology. *Hastings Communications & Entertainment Law Journal, 25*, 653–682.

Fernando, V. (1981). Legal personality, privacy and the family. In Henkin, L. (Ed.). *The International Bill of Rights* (pp. ??–??). New York: Columbia University Press.

findBIOMETRICS.com (n.d.). Hand geometry – now and in the future. Retrieved February 1, 2007, from http://www.findbiometrics.com/Pages/hand_finger%20articles/hand_2.html

Flaherty, D. H. (1999). Visions of privacy: Past, present and future. In C. Bennett & R. Grant (Eds.). *Visions of Privacy: Policy Choices for a Digital Age* (pp. 21–39). Toronto: University Of Toronto Press.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal, 89*, 421–471.

Gomm, K. (2005, October 21). U.K. passport agency: 'Iris recognition needs work'. *ZDNet Asia*. Retrieved July 12, 2006, from http://www.zdnetasia.com/news/security/0,39044215,39283306,00.htm

Grijpink, J. (2004). Two barriers to realizing the benefits of biometrics. Retrieved September 3, 2006, from http://www.cs.uu.nl/people/grijpink/docs/

Harte, A. (2004). Privacy and identity in a changing world. *Australasian Psychiatry, 12*(1), 55–57

Hert, P. D. (2005). Biometrics: Legal issues and implications. Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission. Retrieved January 3, 2007, from http://www.statewatch.org/news/2005/apr/jrc-biometrics-paul-de-hert.pdf

Higgins, P. T. (2003). Fingerprint and hand geometry. In J. K. Brownlow (Ed.), *Biometrics* (pp. 25–41). McGraw-Hill.

Holladay, A. (2002). Do identical twins have identical DNA? Retrieved February 1, 2007, from http://www.wonderquest.com/twins-dna.htm

ICAO. (2004). Biometrics deployment of machine-readable travel documents: Technical Report, Version 2.0. Retrieved February 1, 2007, from http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf

Impagliazzo, R. & More, S. M. (2002). Anonymous credentials with biometrically-enforced non-transferability. Retrieved September 3, 2006, from http://portal.acm.org/ft_gateway.cfm?id=1005150&type=pdf&coll=&dl=ACM&CFID=15151515&CFTOKEN=6184618

Inness, J. C. (1992). *Privacy, Intimacy and Isolation*. Oxford, New York: Oxford University Press.

Jian, A. K., Ross, A., Uludag, U. (2005). Biometric template security: Challenges and solutions. Retrieved June 5, 2006, from http://www.ee.bilkent.edu.tr/~signal/defevent/papers/cr1805.pdf

Kent, S. T. (2006). IDs – not that easy: Questions about national wide identity system. Retrieved February 1, 2007, from http://www7.nationalacademies.org/ocga/testimony/IDs_Not_That_Easy.asp

Kenyon, L. D. (n.d.). Five years later ... Airport video technologies evolve in wake of 9/11. Retrieved September 4, 2006, from http://governmentvideo.com/articles/publish/article_962.shtml

Keogh, E. (2001). An overview of the science of fingerprints. *Anil Aggrawal's Internet Journal of Forensic Medicine and Toxicology, 2*(1). Retrieved January 4, 2007, from http://www.geradts.com/anil/ij/vol_002_no_001/papers/paper005.html

Laitner, S. & Williamson, H. (2005, November 9). E-passport is no laughing matter. *Financial Times*. Retrieved February 1, 2007 from http://www.ft.com/cms/s/d51ee8d0–50c6–11da-bbd7–0000779e2340.html

Lawless, J. (2004). Fingerprint privacy concerns. *CBS News*. Retrieved September 4, 2006, from http://www.cbsnews.com/stories/2004/09/08/tech/main641998.shtml

Leyden, J. (2004, May 26). FBI apology for Madrid bomb fingerprint fiasco. *The Register*. Retrieved August 10, 2006, from http://www.theregister.co.uk/2004/05/26/fbi_madrid_blunder/

Lin M. (1996). Conferring a federal property right in genetic material: Stepping into the future with the Genetic Privacy Act. *American Journal of Law and Medicine, 22*, 109–134.

McCoy, S. (2002). Comment: O' big brother where art thou? The constitutional use of facial-recognition technology. *John Marshall Journal of Computer & Information Law, XX*(3), 471–???

Moo-Young, R. (2001). Eyeing the future: Surviving the criticisms of biometric authentication. *North Carolina Banking Institute, 5*(Spring), 421–435.

National Institute of Standards and Technology. (2001). Common biometric exchange file format (CBEFF) (NISTIR 6529). Retrieved June 3, 2006, from http://www.itl.nist.gov/div895/isis/bc/cbeff/CBEFF010301web.PDF

Norman, D. (2003). Don Norman's jnd.org: Recommended readings. Retrieved February 1, 2007, from www.jnd.org/recommended_readings.html (reviewing Bruce Schneier, *Secrets & lies: Digital security in a networked world*).

O'Neill, R. (2005, August 2). IDologists. *Sydney Morning Herald*. Retrieved February 1, 2007, from http://www.smh.com.au/news/next/idologists/2005/08/01/1122748570079.html?oneclick=true

Ploeg, I. (1999). Written on the body: Biometrics and identity. *Computers and Society*, March, 37–44.

Retica Systems Inc. (2005). Eye biometrics. Retrieved September 6, 2006, from http://www.retica.com/site/biometrics/index.html

Rinehart,G. (2001). Biometric payment: The new age of currency. *Hospitality Upgrade Magazine*, Spring. Retrieved December 1, 2006, from http://www.hotel-online.com/News/PressReleases2000_1st/Mar00_BiometricCurrency.html

Rothstein, M. A. (Ed.). (1997). *Genetic Secrets: Protection of Privacy and Confidentiality in the Genetic Era*. Yale: Yale University Press.

Rotenberg, M. A. (2002). Joint hearing on identity theft involving elderly victims before the special committee on aging. Retrieved September 7, 2006, from http://www.epic.org/privacy/biometrics/testimony_071802.html

Roy, B. (2005). A case against biometric national identification systems (NIDS): «Trading-off» privacy without getting security. *Windsor Review of Legal and Social Issues, 45*(March), 59–61.

Scanlon, T. (1975). Thomson on privacy. *Philosophy & Public Affairs, 4*, 315–322.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*, New York: John Wiley & Sons.

Schneier, B. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

Scottish Criminal Record Office. (2002). History of fingerprints – a timeline. Retrieved June 21, 2006, from http://www.scro.police.uk/fingerprint_history.htm

Stoney, D. A. (1997). Fingerprint identification: Scientific status. In D. L. Faigman, D. H. Kaye, M. J. Saks, & J. Sanders (Eds.). *Modern scientific evidence: The law and science of expert testimony*, (pp. 368–399). St Paul, MN: West Publishing.

Thomson, J. J. (1975). The right to privacy. *Philosophy and Public Affairs, 4*, 295–314.

Turley, J. (2000, January 9). National ID: Beware what you wish for. *Los Angeles Times*. p. B.13.

US Fed News Service (2006). Australia: Smartcard for Surveillance, Including US State News, Washington, D.C. June5, 2006

Vandervelde, K. (1980). The new property of the nineteenth century: The development of the modern concept of property. *Buffalo Law Review, 29*, 325–???

Warren, S. & Brandeis, L. (1890–91). The right of privacy. *Harvard Law Review, 4*, 193–220.

Watson, J. D. (2004). *DNA: The Secret of Life*. New York: Knopf.

Wayman, J. L. (1998 May). *Biometrics in Human Services*, *vol2*, No, 2

Wayman, J. L. (2000a). A definition of «biometrics». In J. L. Wayman (Ed.). *National Biometric Test Centre Collected Works 1997–2000* (pp. 21–23). San Jose State University. Retrieved February 1, 2007, from http://www.engr.sjsu.edu/biometrics/nbtccw.pdf

Wayman, J. L. (2000b). When bad science leads to good law: The disturbing irony of the *Daubert* hearing in the case of *U.S. v. Byron C. Mitchell*. Retrieved February 1, 2007 from http://www.engr.sjsu.edu/biometrics/publications_daubert.html

Wayman, J., Jain, A., Maltoni, D., Maio, D. (2004). *Biometric systems: Technology, design and performance evaluation*. London: Springer.

Westin, A. F. (1970). *Privacy and Freedom*. New York: Atheneum.

Wilson, S. & Prints, T. (2004, August 14). *New Scientist*. Retrieved August 13, 2006, from www.newscientist.com/aricle.ns?id=mg18324604.200.

Wilson, S. (2005). Lockstep Submission to Senate Privacy Inquiry. Retrieved August 26, 2006, from http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/submissions/sub11.pdf (pp.12–20).

Woodward, J. D. (1997a). Biometrics: Identifying law & policy concerns. Retrieved June 12, 2006, from http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf

Woodward J. D. (1997b). Biometrics: Privacy's foe or privacy's friend? *Proceedings of the Institute of Electrical and Electronics Engineers, 85*(9), 1480–1492.

Woodward, J. D. (2001a). *Super bowl surveillance: Facing up to biometrics*, Rand Issue Paper 209. Retrieved February 1, 2007, from http://www.rand.org/pubs/issue_papers/2005/IP209.pdf

Woodward, J. D., (2001b). *Army biometric applications: Identifying and addressing socio-cultural concerns*, RAND Corporation

Zetter, K. (2006, August 3). Hackers clone e-passports, *Wired*. Retrieved February 1, 2007, from http://www.wired.com/news/technology/0,71521–0.html?tw=rss.technology

NÅR HØYESTERETT IKKE FINNER LOVEN

Gert-Fredrik Malt

1 Innledning

1.1

Loven er vår viktigste rettskilde, lovbestemmelser styrer våre liv. Det synes da også å være et rimelig krav, særlig til oss jurister, at vi har oversikt over dem, at vi vet *hvilke* som finnes, og *hvor* vi skal finne dem, når vi trenger dem.

For *ikke-jurister* kan dette virke som en umulig oppgave – den store røde lovboken fremstår i seg selv som en ugjennomtrengelig materie. For *jurister* er det stort sett ikke så vanskelig: Vi lever et liv blandt paragrafer. Vi tar det som en selvfølge å slå opp i lovsamlingen; noe av det første vi lærer er å finne og bruke lovbestemmelser. De viktigste lovene kjenner vi, andre har vi hørt om, og om vi er på et fremmed rettsområde vet vi at vi kan bruke lovsamlingens registre, eller Lovdata. Stort sett går det greit. Det vi er opptatt av er lovens eller lovbestemmelsens *innhold*, – hvordan den skal *forstås,* ikke at den *finnes*.

Men kanskje nettopp fordi vi tar loven – og aller mest lovene på vårt eget rettsområde – som en selvfølge, hender det at vi som jurister under lesningen av en dom *stusser, og tenker*: Jamen – *hva med x-lovens § y*? Fører ikke den til et annet resultat? *Har domstolen oversett bestemmelsen*? Særlig påfallende er dette når saken har vært i Høyesterett, og vi ved lesning av dommen ikke finner *vår paragraf*. Kan det virkelig være at Høyesterett selv ikke har funnet loven – *den avgjørende lovbestemmelsen*?

Ja, det kan faktisk skje. Jeg skal her gi noen små eksempler, og mulige forklaringer på at loven er blitt oversett, i tillegg til at jeg vil si noe om hva dette innebærer, praktisk. Men først må noe mer sies om hva slags tilfeller vi leter efter, og hva som ikke bør regnes med. Og jeg kan si allerede nå, at det vi ender med, ikke er så dramatisk som tittelen kan tyde på. Satt på spissen: Når Høyesterett ikke finner loven, er det oftere loven det er noe galt med, enn Høyesterett. Og emnet handler mindre om de store rettsspørsmål enn om finjussens grenser.

At en lovbestemmelse ikke finnes når den kunne vært anvendt, er ett av flere eksempler på *mangelfull rettsfinning* (her: lovfinning). Et underliggende

spørsmål vil være hva den manglende lovfinningen *skyldes,* og hva som eventuelt kan gjøres for å hindre at noe slikt skjer.

1.2

Jeg vil konsentrere meg om tilfeller hvor unnlatelsen skjer i *sivile tvistemål,* og i *Høyesterett* eller i *Høyesteretts ankeutvalg* (tidligere: kjæremålsutvalget). I noen utstrekning vil jeg også omtale advokaters og andre rettsfinneres forsømmelser; men at disse kan overse lovbestemmelser og andre rettskilder, særlig utenfor deres eget vanlige arbeidsområde, er mer forståelig – og noe av det som gjør arbeidet som jurist utfordrende. Høyesterett må man derimot kunne vente mer av. Og domstolene har en selvstendig plikt til å finne og kjenne rettsreglene; se tvistel § 11–3 første punktum (tidligere tvml § 191).

Jeg vil også konsentere meg om tilfeller hvor det som overses er en *bestemmelse i en formell norsk* (innennasjonal) *lov*. At endog Høyesterett, bl.a. pga partenes manglende medvirkning, kan overse *andre rettskilder* er mindre oppsiktsvekkende, selv om også det kan være beklagelig nok. Dette kan ramme både forskrifter og andre regelverk, tidligere dommer, private avgjørelser, juridisk litteratur, fremmed rett, folkerett – herunder bestemmelser i menneskerettskonvensjoner og EØS-rett – og selvfølgelig reelle hensyn; samt forskjellige former for uskreven rett. Men at en formell norsk lov overses er mer skandaløst enn alt dette.

Jeg forutsetter også at vedkommende lovbestemmelse faktisk *gjelder for saken* (ville gjeldt for den)*,* typisk ved at den *tilsier* (gir eller taler for) *en særlig løsning* av et spørsmål i den – og forsåvidt at bestemmelsen nå, i etterpåklokskap, er fremfunnet, og tilordnet et visst innhold. Jeg unnlater med dette å drøfte mange andre og vanskelige spørsmål, f.eks. om den rette *tolkningen* av bestemmelsen, om tilfeller hvor man ved begrunnelsen for et standpunkt har *valget mellom* forskjellige begrunnende (hjemlende) *bestemmelser*; samt om tilfeller hvor man i ettertid måtte mene at Høyesterett har misforstått forholdet mellom flere bestemmelser og derfor brukt en annen enn den rette. (Se likevel noe om dette i pkt 2 og 4.)

Jeg forutsetter at rettsanvendelsen er innenfor eller forenlig med partenes *anførsler* (påstandsgrunnlag), se tvl § 11–2, jfr § 11–4. Jeg forutsetter også at det ikke finnes andre, ytre formelle hindre for en mer grundig rettsfinning.

Eksemplene vil særlig bli hentet fra det rettsområde jeg selv kjenner best og der jeg er best i stand til å vurdere andres rettsanvendelse: norsk *husromsrett*; og herunder igjen særlig fra norsk *husleie-, boligsamvirke-* og *eierseksjonsrett*. Den tidligere *husleielov*, lov 16/6–1939 nr. 6, vil jeg vise til som *husl 39*; någjeldende lov 27/3–1999 nr. 17, vil jeg vise til som *husl 99*. Den eldre

borettslagsloven, lov 4/2–1960 nr 2 vil jeg omtale som *borl 60;* den nye loven av 4/7–2003 nr. 47 vil bli omtalt som *borl 03*. Den eldre *eierseksjonsloven,* lov 4/3–1983 nr. 7 vil jeg omtale som *eisl 83;* den någjeldende lov 23/5–1997 nr. 31 vil jeg omtale som *eisl 97*.

I noen tilfeller vil jeg vise til min egen omtale av sentrale husromsrettslige domstolsavgjørelser i tidsskriftet *Nytt i privatretten* (forkortet: *NiP*), der jeg redegjør mer inngående for den enkelte avgjørelse og for dens lovanvendelse.

1.3

Formålet med artikkelen er ikke å gi en inngående og systematisk, empirisk eller rettskildedogmatisk redegørelse for emnet, men det mer beskjedne: dels å få frem emnet selv og sannsynliggjøre at manglende lovfinning overhodet *forekommer*, og samtidig å antyde noen mulige *forklaringer* på fenomenet, og *følger* av det.

De fleste domstolsavgjørelsene og andre eksempler jeg nevner vil gjelde *små og ofte enkle rettsspørsmål*. Som hovedeksempler vil jeg bruke tre avgjørelser gjengitt henholdsvis i *Rt 1997 s. 282* (se nærmere særlig i pkt 4.4, 5.3 og 5.4), *Rt 1999 s. 1755* (se særlig pkt 4.2 og 4.4), og *Rt 2008 s. 976* (se særlig pkt 4.4). Jeg skal også nevne noen andre tilfeller, herunder noen lovbestemmelser som lett *kan bli oversett,* uten at jeg har registrert tydelige eksempler på at det har skjedd. Det som er blitt eller kan bli oversett i de tilfellene jeg omtaler er mest perifere lovbestemmelser, og noen stor trussel mot rettssikkerheten er unnlatelsen følgelig ikke. Men i den enkelte sak, for den som rammes av feilen, kan følgen bli viktig nok; se pkt 5. Og for den som vil vite hvordan rettssystemet virker, er det viktig å vite også hva som ikke gjør det, og grunnene til det.

Jeg hører gjerne fra lesere som har andre og bedre eksempler enn dem jeg gir.

2 Taushet om loven trenger ikke bety at loven er oversett

Om man mener å ha oppdaget at en lovbestemmelse er oversett av Høyesterett, er det viktig å ikke være for raskt ute med en fordømmelse. Dette gjelder vel som en praktisk regel overhodet, men ved lesning av Høyesteretts dommer er mistankens hermeneutikk særlig malplassert. Stort sett er en *ydmykhetens hermeneutikk* mer passende. Høyesterett består av fem høyt kvalifiserte jurister, som kanskje har studert saken i dagevis, ledsaget av advokater, med bakgrunn i både tidligere dommer og andre dokumenter. Det er en god sjanse for at de har tenkt og sett lengre enn en selv; og det er ikke gitt at dommerne sier høyt alt de har tenkt.

En skoleriktig påvisning av en oversett lovbestemmelse vil kanskje bli møtt med et skuldertrekk av den dommeren det gjelder, idet han/hun sier: Jovel, det stemmer *forsåvidt* at bestemmelsen kunne vært nevnt og gjelder her; men jeg valgte å fremheve det sentrale, heller enn det selvfølgelige.

Det kan være mange *gode grunner til at en lovbestemmelse ikke finnes* i referatet av en dom eller i dommen selv, uten at det uten videre betyr at bestemmelsen er blitt oversett av domstolen.

2.1

At *hodet* til dommen (Retstidendes kortreferat) ikke nevner en bestemmelse, er selvsagt ikke avgjørende; det avgjørende er teksten selv.

Det er vanlig at hodet ikke nevner alle lovbestemmelser som avgjørelsen faktisk inneholder; og det forekommer også at dette endog gjelder for presentasjonen i Lovdata. Særlig viktig er det å huske dette i tilfeller hvor dommen eller foravgjørelser til den bare er gjengitt med hodet (som kortreferat) i Rt eller RG; se nedenfor.

2.2

Selv om en lovbestemmelse ikke er direkte omtalt/henvist til i avgjørelsen selv, kan det være at domstolen likevel har forholdt seg bevisst til den.

Mest opplagt virker dette i tilfeller hvor vedkommende lovbestemmelse riktignok ikke er uttrykkelig omtalt av Høyesterett, men *den finnes i en av de tidligere avgjørelsene i saken*. Dette gjør at man praktisk kan ta for gitt at også Høyesterett har lagt merke til bestemmelsen. I Norsk Retstidende finnes mange eksempler på dette; noe man ikke alltid blir klar over om man bare leser avgjørelsen selv eller det som står om den i Retstidende eller i Lovdata.

Et eksempel gir den eneste dommen av Høyesterett om husl 39 § 28 (se nå husl 99 § 5–4 tredje ledd 2 pkt): *Rt 1958 s. 1367*. Både i Rt og i Lovdata gjengis dommen bare ved kortreferat. Ved nærmere undersøkelse viser seg at det eneste stedet lovbestemmelsen uttrykkelig nevnes er i *byrettens dom* (som bare er tilgjengelig fra Statsarkivet i Tromsø). Men det at bestemmelsen omtales der, gjør at Høyesteretts dom får et tydeligere innhold.

At det ikke vises uttrykkelig til en bestemmelse er også praktisk ved *særlig hyppig brukte bestemmelser,* der anvendelsen av bestemmelsen er selvfølgelig. Jeg har inntrykk av at dette er mest utbredt i *sivil- og straffeprosess*, der man ofte – strengt tatt – i løpet av saken må anvende en lang rekke forskjellige bestemmelser for å løse praktiske prosesspørsmål.

En unnlatt påberopelse kan også skyldes at bestemmelsen har et så *vidt innhold og anvendelsesområde* at anvendelsen av den i enkelttilfeller ikke lenger beror på en fintolkning av ordlyden, men på rettskilder utenfor den – hvorved det er disse som blir trukket frem og diskutert, heller enn bestemmelsen selv; og hvor det kan virke overdrevent omstendelig å måtte vise til bestemmelsen. Også det at bestemmelsen i sitt hovedinnhold som bakgrunnsretten på området, gjør at det virker unødvendig å vise til den.Et praktisk eksempel på dette i husleieretten, gir mange avgjørelser om *husbråk* og annen overtredelse av husordensreglene som grunnlag for oppsigelse eller hevning, efter tidligere husl 39 § 38, jfr § 22 – se nå husl 99 § 9–5, jfr 9–8 og § 5–2; se som eksempel *Rt 1980 s. 29* (s. 36. § 22 er imidlertid er nevnt i byrettens dom). Det samme gjelder for mange avgjørelser om overtredelse av andre *brede leietakerplikter*, f.eks. efter husl 39 §§ 20 eller 24 første ledd – nå husl 99 § 5–1 annet ledd og tredje ledd første punktum. Et eksempel på mye av dette gir *Rt 1972 s. 1032*, der (visstnok, ifølge referatene i Rt) ingen av instansene, ved vurderingen av luktulemper fra leietakers virksomhet, forholdt seg åpent til disse bestemmelsene. Et annet eksempel kan være avgjørelser om utslukkelse av rettigheter ved manglende *tinglysning* av dem efter tgl §§ 20 og 21 – der domstolen ofte vil unnlate å vise uttrykkelig til bestemmelsene; se som eksempel også her *Rt 1980 s. 29* (s. 34 flg).

Også anvendelse av visse rettsovergripende *rettslige standarder* antar jeg kan gi eksempler på dette.

Også ellers kan det nok forekomme tilfeller hvor både *resultatet og begrunnelsen i en sak virker så opplagt*, at det ikke synes nødvendig å nevne uttrykkelig den bestemmmelse det angår.

2.3

Det bør ikke regnes ikke som mangelfull lovfinning overhodet (i denne artikkelens forstand), om Høyesterett synes å ta feil i *valget av hjemmelsbestemmelse* for et standpunkt, i tilfeller hvor det mer eller mindre åpenbart kan anføres flere slike. Dette er en type begrunnelsesfeil som er mer utbredt enn de tilfellene jeg her omtaler.

Slike valg som her nevnt kan kanskje betegnes som *hjemlingsfeil*. Men det kan diskuteres hva som overhodet skal regnes som «feil» i slike tilfeller. Ofte er det mer treffende å forstå forholdet som saklig-teknisk tolknings*uenighet*, enn som et spørsmål om riktig/galt.

Et eksempel i fleng på mye av dette, gir *Rt 2004 s. 1385*, der Høyesteretts kjæremålsutvalg i et utkastelsessak løste spørsmålet om hvorvidt andel av fellesutgifter til en felles telefontjeneste var «leie» efter *tvfl § 13–2 tredje ledd pkt*

a, men bare ut fra den bestemmelsen, uten å drøfte forholdet til husleielovens alminnelige regler om dette i husl 99 kap 3; særlig § 3–1 første ledd og § 3–4 (med dennes tredje ledd), eller forsåvidt ut fra fra borl 60 (særlig §34, jfr § 36, men eventuelt også §§ 46 og 54).

Et annet eksempel, gir *Rt 2004 s. 1785,* om saksøktes mulighet for å avbryte et påbegynt tvangssalg ved betaling av det underliggende kravet efter *tvfl § 5–17 første ledd pkt a*. Kjæremålsutvalget konsentrerte her sin drøftelse om *borl 60 § 27, jfr § 18*, noe som antakelig bidro til at mulighetene ble oversett for en forståelse av løsningen som gitt ved utvidende tolkning av § 5–17 selv. (Dette og andre spørsmål om lovanvendelsen i saken er omtalt av meg i NiP 2005/2, s. 10–11.)

3 Kan vi vite om Høyesterett har oversett noe?

Et spørsmål generelt om unnlatelsessynder, er om og evt hvordan vi overhodet kan vite om et handlende subjekt, at det ikke har tatt noe bestemt i betraktning. Praktisk er dette et spørsmål om hva vi skal ha som tegn på at det er eller ikke er tilfelle. Kan vi overhodet *vite* det, om Høyesterett har oversett en lovbestemmelse? Kanskje ikke. Men det vi kan finne er at *mye tyder på* at det er tilfelle.

Selv ut fra en velviljens hermeneutikk som nevnt, er det ingen grunn til å innrømme Høyesterett noen immunitet mot enhver mistanke. Også Høyesterett må finne seg i å bli vurdert efter det domstolen og dens dommere faktisk sier, ikke efter en ide om hva de egentlig ville være i stand til å si. Og om det i eftertid viser seg at vi tok feil i kritikken, kan vi fremdeles insistere, nå på en *begrunnelseskritikk:* Vi kan mene at domstolen i det minste *burde vist til* lovbestemmelsen.

3.1

Problemet kommer som sagt ovenfor (pkt 2) først på spissen når *vi ikke finner en uttrykkelig henvisning* til en lovbestemmelse vi selv har funnet frem til og som vi mener må være av betydning for saken; dvs at bestemmelsen *ikke er nevnt på noe stadium i saken,* hverken i avgjørelsens *hode*, i *avgjørelsen selv* eller i *tidligere avgjørelser*.

3.2

For å være sikker, burde vi strengt tatt også undersøke andre ikke offentlige *dokumenter* i saken, så som *utdragene* for Høyesterett og partenes *prosesskrifter.* Ideelt sett kunne vi kanskje gå enda lenger, f.eks. ved uttrykkelig å

spørre dem det gjelder, både partene, deres prosessfullmektiger og dommerne i saken, om de har *vurdert og evt sagt noe om* anvendelsen av vedkommende lovbestemmelse. Men om en slik ytterste granskning ikke lar seg gjennomføre, må utgangspunktet være at vi vurderer de uttalelsene som faktisk foreligger, i avgjørelsene selv.

Jeg selv pleier ved omtale av dommer til Nytt i Privatretten å kontakte *prosessfullmektigene* for å høre nærmere om deres anførsler, prosedyre og inntrykk av saken; og ved omtalen her av Rt 1997 s. 282 og av Rt 2008 s. 976 bygger jeg bl.a. på dette. (Om den siste avgjørelsen, se NiP 2008/3). Men en slik aktiv undersøkelse er tidkrevende – og i praksis ikke alltid heller teknisk mulig. Å spørre *høyesterettsdommerne* selv har jeg hittil ikke gjort – kanskje mest for å unngå å sette på spissen spørsmål om forholdet mellom erindring, efterpåklokskap og dommernes og domstolens prestisje.

3.3

Å kritisere domstolene for å ha oversett en lov kan virke som en *freidig etterpåklokskap*, som bare er mulig i den utstrekning vi selv mener å ha bedre oversikt over rettskildebildet enn domstolen. Er dette noe vi overhodet kan tillate oss? Efter min mening er det *noe vi ikke kan unngå*, iallfall når vi nærmer oss domstolenes avgjørelser med et bevisst rettsvitenskapelig og metodisk systematisk blikk. At vi kan ha svakheter i vår egen juridiske metode bør ikke hindre oss i å påpeke svakheter i andres.

3.4

De sikreste tegnene når det gjelder innholdet, er mangler ved avgjørelsens begrunnelse eller ved dens resultat, som gir avgjørelsen selv en *ensidighet*.

Det vi gjerne først legger merke til ved slike avgjørelser, er at *begrunnelsen* fremstår som mangelfull, og at den *ville blitt en annen*, selv for samme resultat, dersom den oversette bestemmelsen var tatt med.

I noen tilfeller fører mangler ved begrunnelsen til at vi går enda lenger: Vi føler at selve *resultatet* (utfallet i saken) med en viss sannsynlighet (sikkert, høyst sannsynlig, sannsynlig, kanskje) *ville blitt et annet*; – dersom den oversette bestemmelsen var tatt i betraktning.

I slike tilfeller må vi kunne våge å tenke og si det høyt: at vedkommende bestemmelse er blitt oversett, og at den burde vært tatt i betraktning.

4 Noen grunner til at lovbestemmelser blir oversett, med eksempler

En domstol kan ha mer eller mindre gode *grunner for å overse* en lovbestemmelse, noe som ofte springer ut av egenskaper ved lovbestemmelsen selv. Her vil jeg si noe om dette, samtidig som jeg gir noen eksempler. Noe som typisk kjennetegner bestemmelser som blir oversett, er at de er *sjeldne, bortgjemte* og/eller at de har et *særegent innhold*. I praksis vil gjerne flere av grunnene foreligge samtidig og befeste hverandre. Til dette kommer typisk særlige *forventninger* hos domstolene som gjør at de lettere *nøyer seg* med det de allerede har, uten å lete efter bestemmelser de ikke vet om.

4.1

Aller først: En praktisk medvirkende grunn til at domstolene overser loven, er alltid at *partenes prosessfullmektiger* har unnlatt å påberope vedkommende lovbestemmelse. I slike tilfeller kan det sies at domstolene ikke alene har skylden. En annen praktisk grunn, kan være *tidsnød* hos domstolen; f.eks. fordi man bare viser saken og rettsfinningen i den den tid man *tror* den trenger, uten å bruke den tid som egentlig trengs. Men noen god unnskyldning er alt dette ikke, gitt *den selvstendige plikt domstolen har til å finne og anvende gjeldende rettsregler* (se pkt 1.2).

4.2

En første reell situasjon hvor en lovbestemmelse kan bli oversett, har man i *overgangstilfeller,* hvor en lovbestemmelse *fremdeles eller midlertidig er gjeldende rett*, men den er i ferd med å bli *foreldet,* og derved risikerer å bli *glemt*.

Jeg bruker ordet *foreldet* her i en vid forstand, hvor lovbestemmelsen fremstår som *gammel, gammeldags* eller *avleggs* på andre måter, sammenlignet med regler som ellers gjelder på området – og som typisk er nyere eller forøvrig virker mer moderne enn vedkommende bestemmelse; gjerne hvor bestemmelsen også er i ferd med å bli erstattet formelt av en ny gjeldende regel.

Lettest forståelig er glemselen i tilfeller hvor det allerede finnes *en nyere lovbestemmelse* som er i ferd med å avløse den gamle, men hvor det likevel er aktuelt å anvende den gamle på vedkommende rettsforhold. Flere av eksemplene nevnt nedenfor her i pkt 4 gir eksempler på dette; se f.eks. *Rt 1999 s. 1755* om ikke- anvendelsen av den gamle *husl 39 § 51 femte ledd* til fordel for både alminnelige og nyere rettsnormer, og også *Rt 2008 s. 976* , der den gamle *borl 60 kap 5* ble oversett, til fordel for de nyere reglene om overføring av fast eiendom i avhendingsloven.

Også flere tradisjonelle eksempler på bortfall av lovbestemmelser *på annen måte enn ved ny lovgivning*, så som ved *ikke-bruk* (desuetudo), kan antakelig regnes som eksempler på dette; se pkt 5.2.

Glemsel kan også inntreffe i tilfeller hvor den oversette bestemmelsen er gitt *midlertidig*, eller som tillegg til en allerede *opphevet lov*, og derfor ikke er tatt opp i rettsanvendernes bevissthet, og kanskje heller aldri kommer inn i lovsamlingen, før den skal anvendes. Eksempler på det siste gir to endringer av *husl 39* efter opphevelsen av denne i 1999: dels endringen av *§ 35* ved lov 31/3–2000 nr. 20, og dels tilføyelsen av et nytt tredje ledd i *§ 42,* ved lov 6/6–2003 nr. 39.

Ofte vil bestemmelser som her nevnt samtidig være *bortgjemt* i eldre eller andre spesielle, *lite brukte lover*, se neste avsnitt.

4.3

En annen situasjon hvor en lovbestemmelse kan bli oversett, er hvor den er *bortgjemt;* ved at den fysisk og systematisk befinner seg på et uventet sted i systemet av lover – og i lovsamlingen, dvs *i en annen lov eller et annet sted i loven*, enn der den efter sitt innhold i utgangspunktet burde være – gjerne fordi bestemmelsen handler om noe annet enn det den loven hvor den finnes ellers handler om.

Også ordet *bortgjemt* bruker jeg her i en vid forstand; om forskjellige former for praktisk *utilgjengelighet*.

Mest typisk er tilfeller hvor lovbestemmelsen befinner seg i en egen (og kanskje gammel) og lite brukt *særlov*, eller på et særlig *sted i en lov*, hvor man ikke venter å finne den. Lovsamlingen («Norges Lover») har inneholdt mange artige eksempler på dette, dvs på mer eller mindre fysisk og systematisk bortgjemte lovbestemmelser, som man i praksis må vite om eller må lete særlig efter for ikke å overse. Det virker likevel som dette er lovbestemmelser som sjelden overses helt av domstolene – enten fordi de fremstår som så aparte at en god jurist legger merke til dem – eller fordi de er så viktige på sitt delområde, at man aktivt oppsøker dem. Men jeg antar det finnes tilfeller jeg ikke vet om, hvor bestemmelsen ikke er blitt påberopt og anvendt efter sitt innhold.

Et eksempel på en bestemmelse av denne art utenfor husromsretten gir ennå idag *strl 1902 § 400 første ledd* om allemannsretten til å plukke ville bær osv i utmark, og samme bestemmelses *annet ledd* med hovedregelen om forbudet mot multeplukking i Nord-Norge. Til 31/12–2003 fantes også en egen liten lov om forbud mot plukking av *moltekart* – lov 6/6–1970 nr. 25. Et eksempel fra husromsretten gir de særlige reglene om *boligaksjeselskaper,* f.eks. i tidligere borl 60 § 90 tiende ledd, eller i husl 39 § 42 tredje ledd. Et nyere

pussig eksempel, gir den midlertidige regelen inntatt i *husleiereguleringslovens* (lov 7/7–1967 nr. 13) *§ 15 første ledd femte punktum*, efter en lovendring i 1999, om *husleienemndenes kompetanse* ved tvister om husleiens størrelse, ikke bare efter husl 39 § 35 (slik overskriften til kapitlet tilsier), men også efter husl 99 § 3–1 og 4–3.

Umiddelbart kan det synes som denne grunnen til at bestemmelser oversees ikke lenger er like aktuell idag, ved bruk av et *elektronisk søkesystem* så som ved søk i *Lovdata*; idet slike systemer nettopp ikke er avhengig av en bestemt plassering av lovbestemmelsen, bare av at den lar seg gjenfinne med bruk av riktige *søkeord*. Men det kan også være at gjenfinningsproblemet bare er blitt forskjøvet: Det er nå ikke lenger snakk om *fysisk* bortgjemthet. Men bestemmelsen kan være *språklig* og *systematisk utilgjengelig* på en måte som vanskeliggjør en elektronisk søkning efter den. Det hjelper ikke om det man søker ligger like for nesen på en – sålenge man ikke finner de rette ordene for å søke efter det.

En variant av dette har man i tilfeller hvor hvor domstolen unnlater å forholde seg til mer *perifere lovbestemmelser om bispørsmål* i en sak som angår en rekke større og mindre delspørsmål, hvor, billedlig talt, den uteglemte lovbestemmelse fremstår som en pølse i slaktetiden. Et eksempel på dette gir kanskje den manglende omtale av *husl 39 § 18 fjerde ledd*, i den store saken om Glasmagasinets ombygging, i *Rt 1998 s. 1980*. Saken kom der først og fremst til å handle om husl 39 § 27; men deler av saksforholdet kunne også vært ført inn under § 18 fjerde ledd.

4.4

En tredje og dypere grunn til at en lovbestemmelse blir oversett, kan være lovbestemmelsens *innholdsmessige særegenhet,* ved at den efter sitt *innhold* fremstår som avvikende eller overraskende, sett på bakgrunn av det man ellers skulle anta som gjeldende rett, f.eks. sett i forhold til alminnelige eller særlige *prinsipper og bakgrunnsretten forøvrig på vedkommende rettsområde*.

I noen slike tilfeller kan det være at lovbestemmelsen blir oversett fordi den krever særlige forutsetninger eller *en særlig lesning for å bli forstått*, og derfor blir oversett av den som ikke stopper opp, dveler ved og finleser den – for å se hva den nærmere inneholder. Et eksempel som delvis kan forstås slik, gir *Rt 2008 s. 976*; der samtlige domstoler overså det regelsettet som først og fremst regulerte forholdet – nemlig borl 60 kap. 5, og herunder særlig § 29, til fordel for alminnelig og nyere bakgrunnsrett – her representert ved avhendingsl § 3–8; om dette se Malt i NiP 2008/3.

Et eksempel gir antakelig også *Rt 2004 s. 1785,* der ingen av instansene synes å ha registrert at strengt tatt heller ikke borl 60 § 27 kunne anvendes direkte i saken, da tvangssalget i saken ikke direkte gjaldt en borettslagsandel, men bare en tildelingskontrakt; se Malt i NiP 2005/2 s. 10.

Det kan også være at domstolen er så sterkt inne i en måte å tenke på knyttet til bakgrunnsretten, at den, på samme måte som andre rettsanvendere, *tar for gitt* at dette også er resultatet på vedkommende felt – uten aktivt å undersøke hvorvidt det er tilfelle; noe som kan føre til at en avvikende lovbestemmelse blir oversett. Noen slike bestemmelser blir omtalt som *feller* i lovgivningen. Husleielovgivningen har inneholdt flere gode eksempler på dette; mest åpenbart i prosessbestemmelser, men også i materiell rett.

Mest beryktet har antakelig vært den lille regelen i *husl 39 § 51 første ledd annet punktum*, om en særlig, kort *ankefrist på 14 dager* i husleiesaker. Dette er en bestemmelse mange advokater har brent seg på, fordi de altfor lett hadde kommet inn i en rutine basert på hovedreglene om ankefrist (tidligere to måneder, efter tidl. tvml 1915 § 360, nå en måned, efter tvl 2005 § 29–5 første ledd). Samtidig har Høyesteretts kjæremålsutvalg ofte vært nådeløs i sin karakteristikk av forsømmelsen som en ikke unnskyldelig rettsvillfarelse, ved å nekte oppreisning mot den efter tidl. domstolsl § 153, med den begrunnelse at det nettopp *kunne legges prosessfullmektigen til last* at han/hun ikke hadde tatt hensyn til bestemmelsen. Denne strenge praksis knyttet til den gamle ankefristregelen ble også opprettholdt ved avgjørelser efter eldre rett i overgangstiden fra gammel til ny husleielov der særregelen ble tatt bort; se inngående om spørsmålet *Rt 2000 s. 505*.

Jeg har ikke foretatt en systematisk gjennomgang av Høyesteretts eller kjæremålsutvalgets egen praksis i husleiesaker, for å finne ut hvorvidt de også selv i alle tilfeller har vært påpasselig med at ankeregelen ble overholdt. Det finnes imidlertid andre tilfeller, der det kan virke som Høyesterett selv har gått i en felle de ellers ikke ville godtatt at andre faller i.

Et slikt tilfelle er *særregelen om saksomkostninger i oppsigelsessaker, i husl 39 § 51 femte ledd*. Ifølge bestemmelsen hadde domstolene en fri adgang til å ilegge eller ikke ilegge saksomkostninger i «oppsigelsessaker etter § 38»; noe som innebar at de vanlige reglene om dette i tvml 1915 kap. 13 ikke – eller iallfall ikke uten videre og skarpt – kom til anvendelse. Men det har hendt at Høyesterett selv har unnlatt å anvende bestemmelsen, nettopp i oppsigelsessaker etter § 38. Et eksempel gir dommen i *Rt 1999 s. 1755*. Til tross for at saken delvis var en oppsigelsessak, ble saksomkostningsspørsmålet avgjort av samtlige domstoler efter tvml kap 13 (§ 172, jfr § 180), uten at husl 39 § 51 femte ledd engang ble nevnt. Til overmål uttalte førstvoterende (s. 1761), at efter avgjørelsen i Høyesterett når det gjaldt gyldigheten av oppsigelsen (der

leietaker tapte) *kunne* ikke leietaker tilkjennes saksomkostninger for denne del av saken for lagmannsretten. Et annet eksempel på det samme, gir *Rt 1997 s. 683*, *jfr Borg LR – Dom 19/8–1996:* Leietaker, som tapte en oppsigelsessak og senere en sak om gjenopptakelse av saken, ble her ilagt saksomkostninger, utelukkende med henvisning til tvistemålslovens alminnelige regler – uten henvisning til husl 39 § 51 femte ledd.

I noen tilfeller er den oversette bestemmelsen strengt tatt ikke innholdsmessig særegen, men heller *selvfølgelig*. Dette gjør at det kan være vanskelig å oppdage, både at den er oversett og konsekvensene av det. Et pussig eksempel gir en kjennelse av Høyesteretts kjæremålsutvalg i *Rt 1997 s. 282*. Saken handlet om et blandet seksjonssameie, der en av bruksenhetene ble brukt som kinolokale, og der boligbrukerne ble plaget av støy fra kinoen, hvorved de, som seksjonseiere, begjærte midlertidig forføyning mot kinoeieren, med krav om at støyen måtte stanses. Saken ble imidlertid ført efter reglene i *granneloven* § 2, jfr § 10 første ledd, anvendt *direkte*, uten at noen av partene eller domstolene oppdaget at hovedregelen for tilfellet heller måtte finnes i *eierseksjonsloven*, nærmere bestemt i daværende *eisl 83 § 11 første ledd* (= nå eisl 97 § 19 annet ledd); og at det også uavhengig av denne var høyst diskutabelt om granneloven overhodet kunne anvendes direkte på forholdet. (Som bakgrunnsrett kunne også vært anført sameiel. § 3.) Se nærmere om tilfellet også nedenfor i pkt. 5.3 og 5.4.

4.5

I praksis vil en lovbestemmelse som blir oversett ofte ha alle de nevnte egenskapene samtidig, ved å være både *foreldet*, *bortgjemt* og *innholdssæregen*.

Begge de nevnte avgjørelsene i Rt 1999 s 1755 og Rt 2008 s. 976 gir et eksempel på dette.

Avgjørelsen i Rt 1997 s. 282 må forklares på en annen måte. Kanskje var det avgjørende i saken at tvisten allerede fra først av ble forstått som en *nabokonflikt*, noe som fikk alle de involverte til utelukkende å tenke på naboloven?

4.6

Noe felles for de tilfellene som er nevnt, synes å være at den oversette lovbestemmelsens egenart foreligger i en situasjon hvor rettsanvenderne – og herunder Høyesterett – samtidig besitter særlige *forestillinger* om hvordan rettstilstanden er, og derved særlige *forventninger* til hva de kan, bør og trenger å lete efter, samtidig som *tvisten selv blir definert* (forstått) ut fra dette.

Det avgjørende i slike tilfeller er ikke at lovbestemmelsen ikke blir funnet av en som leter efter den. Det kan nemlig godt være at regelen *lett ville bli funnet om vedkommende overhodet lette*. Det avgjørende er heller at *domstolen ikke kommer på tanken å lete efter bestemmelsen*, og derfor *lar være å lete*.

5 Noen følger av at en lovbestemmelse overses

Det at en lovbestemmelse overses av Høyesterett kan ha forskjellige følger. Viktigst er de uheldige virkningene rettsanvendelsen kan ha for *partene* i saken – her særlig for den tapende part. Men den mangelfulle lovfinningen kan også ha andre virkninger: for bestemmelsen selv, for andre bestemmelser som kunstig har fått økt sin kraft, for domstolenes omdømme; og dessuten i prinsippet for rettssystemet og rettssikkerheten selv.

5.1

De sakene hvor Høyesterett (tilsynelatende) har oversett en lovbestemmelse kan samlet virke som bagatellmessige. Men de vil ofte være viktige for dem de først og fremst gjelder – for *partene* i saken, og særlig for den av dem som taper – kanskje urettmessig – på grunn av dette.

Rettssystematisk er dette imidlertid neppe hverken verre eller bedre enn andre former for objektivt sett *gale avgjørelser,* hvor avgjørelsen beror på feil faktum eller gal rettskildebruk på andre måter.

5.2

Feil i rettsanvendelsen, – og herunder også unnlatelsen som her av å påberope en aktuell lovbestemmelse – gir ikke grunnlag for *gjenåpning* (gjenopptakelse) av sivile saker. Dette følger dels antitetisk av tvistel 2005 § 31–4 bokstav a, jfr tidligere tvml 1915 § 407 første ledd nr. 6, men dessuten av den alminnelige regelen om at gjenåpning ikke kan begjæres av en grunn som parten burde ha gjort gjeldende under sakens ordinære behandling, se nå tvistel § 31–5 annet ledd, tidligere tvml § 407 annet ledd. Se uttrykkelig om dette i forarbeidene til ny tvistelov, særlig NOU 2001: 32 A s. 447 flg.

I straffesaker og ved anvendelse av folkeretten gjelder tildels særlige regler som jeg her ikke går nærmere inn på; se strprl 1981 § 392 og tvistel § 31–4 bokstav b.

5.3

En naturlig følge av at en lovbestemmelse overses av Høyesterett *for den oversette lovbestemmelsen selv*, kan være at den derefter fremstår med en *svekket kraft;* først og fremst sammenlignet med de reglene som ble anvendt i stedet for den, men eventuelt også sammenlignet med andre regler i rettssystemet.

I noen tilfeller kan dette være et første eller neste skritt i retning av bortfall av bestemmelsen ved *ikke-bruk* (desuetudo). Mange eldre tilfeller av ikke-bruk, og der ikke-bruken ikke skyldes en bevisst tilsidesettelse av bestemmelsen, antar jeg har begynt slik.

Men dette trenger ikke alltid være tilfelle. Det kan også være at den oversette bestemmelsen beholder sin kraft og herefter bare blir forstått på en ny måte, f.eks. *som utslag av den anvendte, mer alminnelige regelen*. Et eksempel på dette gir *Rt 1997 s. 282*. En virkning av avgjørelsen for *eisl 83 § 11 første ledd*, var antakelig at bestemmelsen gjennom avgjørelsen ble *bekreftet som et utslag av grannelovens § 2, forstått som hovedregel*; og også slik at grannel § 2 herefter ville kunne gi momenter ved tolkning av bestemmelsen. En paradoksal følge av dette kan være at den oversette regelen endog får en *større kraft* – ved at den ikke lenger står alene, men *befestes* av den mer alminnelige regelen.

At bestemmelsen er blitt oversett av Høyesterett kan også gi et argument for at det er eller var tillatt for andre å overse den – dvs for anerkjennelse av en manglende kunnskap om bestemmelsen hos rettsanvendere, som en delvis unnskyldelig *rettsvillfarelse*. Men se til dette også pkt 5.2 ovenfor. Det er dessuten vanskelig – og kanskje endog ikke alltid ønskelig? – å være konsekvent her. Det er tankevekkende å sammenligne på den ene side Høyesteretts skarpe reaksjoner mot andres overtredelse av *husl 39 § 51 første ledd annet punktum*, og på den annen side Høyesteretts egne unnlatelser med å anvende samme paragrafs *femte led*d; se ovenfor pkt 4.4.

5.4

Når det viser seg at domstolen ved anvendelse av en lov har uaktsomt oversett en annen, er det samtidig nærliggende å anse *den anvendte loven som svekket* – iallfall i den forstand at prejudikatet for anvendelsen av den i dette tilfellet er blitt det; idet anvendelsen på en måte har vist seg å bero på en villfarelse.

Det er imidlertid også mulig å hevde det motsatte: Det at den nyere, mer åpenbare og mer generelle regelen er blitt anvendt fremfor den eldre, skjulte og innholdssære regelen, kan forstås som en *ytterligere befestelse av den anvendte regelens kraft*; kanskje med virkning også for andre, omkringliggende lovbestemmelser.

Et godt eksempel på dette gir antakelig avgjørelsen i *Rt 2008 s.976*, om salg av nybygde borettslagsleiligheter fra et borettslag med økning av andelskapitalen; der salget ble behandlet efter den nye, spisse regelen i avhendingsl § 3–8, ikke bare på bekostning av borl 60 § 29, men også tildels på bekostning av alminnelige rettsprinsipper, jfr Malt i NiP 2005/3. En følge av dommen kan bli at § 3–8 blir ytterligere befestet som uttrykk for en hovedregel om eiendomsselgeres opplysningsrisiko, og for denne regelen selv.

Det samme kan sies om avgjørelsen i *Rt 1997 s. 282*. At granneloven ble anvendt kan sies å tale for en *utvidende tolkning,* ikke bare av naboloven § 2, men også av anvendelsesområdet for loven overhodet – og derved også for andre særregler i denne, så som den objektive erstatningsregelen i § 9. Hvorvidt dette også vil bli det endelige utfallet av utviklingen avhenger imidlertid også av andre argumenter, og gjenstår å se.

5.5

Det at Høyesterett overser lovbestemmelser kan ha virkninger for *domstolenes alminnelige omdømme*. Men det er ikke klart i hvilken retning dette vil gå.

Hos legfolk kan det nok tenkes at historier om Høyesteretts *feiltrinn* bidrar til å svekke domstolenes og dommernes omdømme. Men efter min mening gir de tilfellene jeg har sett ikke grunnlag for noen egentlig *kritikk* av domstolen. Jeg synes det er mer nærliggende å lese eksemplene som en bekreftelse på at dommerne ikke bare er *mennesker*, men at de nettopp i sin egenskap av høyesterettsdommere er *generalister*, som ikke kan overskue rettssystemet i dets helhet og med alle detaljer.

I en forstand kan man også ta erfaringene *positivt*: Det er godt å erfare at Høyesterett i slike tilfeller synes å havne i *forsvarlige standpunkter*, basert på et inderlig forhold til *bakgrunnsretten*.

5.6

For *advokatstanden* kan historier om mangelfull lovfinning fra Høyesteretts side kanskje som en vitamininnsprøytning, ved at det minner oss alle om hvor viktige prosessfullmektigenes bidrag til rettsanvendelsen er.

6 Avsluttende bemerkninger

6.1

At det overhodet finnes tilfeller hvor Høyesterett ikke finner frem i loven – eller finner frem til riktig lov – skyldes først og fremst det trivielle faktum at retten i en viss utstrekning alltid er og må være *uoversiktlig,* også på den måten at det å finne en *regel som passer* på et rettsforhold kan være både praktisk og prinsipielt vanskelig. Det har å gjøre med selve måten en uendelig mengde normativ informasjon kan og bør stå i forhold til en uendelig kompleks verden på: Retten, og systemet av lover er ikke bare en rekke med regler, ordnet på geledd. Det er regler gitt fra en rekke forskjellige perspektiver, ut fra forskjellige verdier og mål, på forskjellige tidspunkter, med forskjellig abstraksjonsgrad, og i flere lag, svarende til forskjellige aspekter av virkeligheten selv.

6.2

Selv om det kan være vanskelig, klarer vi stort sett *å finne lovbestemmelser som passer*.

For alt dette har vi *registre* og *søkesystemer* av forskjellig art, både trykte og elektroniske, herunder både alfabetiske og kronologiske registre, som gjør det mulig å finne det vi leter efter, når vi trenger det. *Om vi vet noe finnes klarer vi stort sett å finne det*. Men det er ikke alltid vi vet om det som finnes, og vi unnlater derfor kanskje å lete efter det.

Den som leter, finner. Men den som ikke leter, finner ikke. Og jo eldre, jo mer bortgjemt og særegen en bestemmelse er, jo større sjanse er det for at vi unnlater å lete, fordi vi ikke en gang tenker oss muligheten for at den finnes.

6.3

Er det at lovbestemmelser overses en trussel mot *rettssikkerheten?* Jeg mener nei; iallfall ikke så lenge det ikke ligger mer i forholdet enn det som er nevnt, og så lenge alle involverte, både partene, deres prosessfullmektiger og domstolens personale gjør hva de kan for å unngå slike feil.

6.4

Kan og bør noe gjøres for å forbedre lovfinningen?

Noe ligger i det som er sagt: Å holde *lovene selv* oppdatert, å la lovbestemmelser finnes der hvor vi venter å finne dem, å ha et bevisst, kanskje aktivt flaggende forhold til innholdssæregne bestemmelser.

Hva mer? Kanskje bare dette: Å minne om dette som en *utfordring:* at vi som jurister *ikke må ta noe for gitt* – at vi alltid, og særlig i sjeldne sakstyper, bør tenke oss om, bruke vår juridiske fantasi, og spørre *hvorvidt det kan finnes særlige lovbestemmelser* som regulerer spørsmålet. I noen slike tilfeller får man overraskende napp.

En god lovbruker skal kunne finne frem, også til lover og lovbestemmelser man ikke vet om. Men om Høyesterett ikke finner loven, er det noe vi alle bærer ansvaret for.

REGULERING AV E-POST SOM BEVIS ETTER DEN NYE TVISTELOVEN – PRAKTISKE OG RETTSLIGE UTFORDRINGER*

Maria Astrup Hjort

1 Innledning

Den 1. januar 2008 trådte lov om mekling og rettergang i sivile tvister (tvisteloven) av 17. juni 2005 nr. 90 i kraft. Loven erstatter tvistemålsloven av 1915 og er den viktigste reform av norsk sivilprosess i moderne tid. I denne artikkelen skal jeg behandle noen sentrale bestemmelser i den nye loven knyttet til håndtering av e-post som bevis. Artikkelens intensjon er å gi en oversikt over hvilke bevisregler som gjelder; hva som videreføres fra tvistemålsloven og hvilke regler som er nye. Artikkelen gir også et innblikk i situasjoner der e-post som bevis gir utfordringer som ikke er vurdert i forarbeider eller lovkommentar.

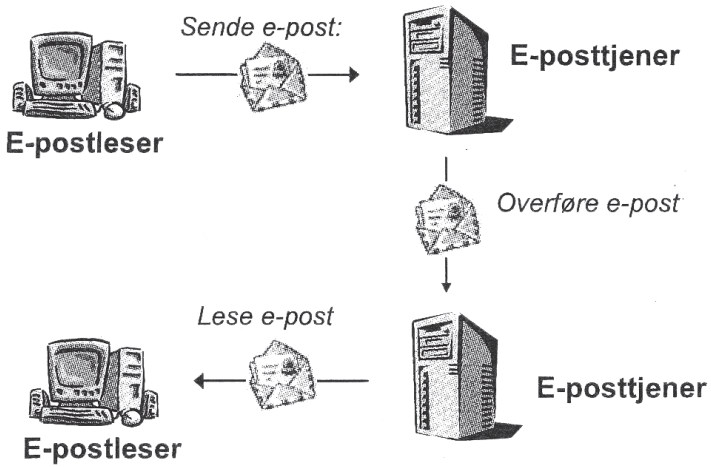
2 Om e-post som teknisk fenomen[1]

En e-post er en tekstfil bestående av et meldingshode og en meldingskropp («header» og «body»). Meldingshodet angir mottaker og avsender av meldingen, tittel og tidspunkt for når meldingen ble sendt. Meldingskroppen er selve innholdet i e-posten.

---

* Artikkelen er tidligere publisert i Festskrift til Jussformidlingens 35-årsjubileum. – Bergen : Jussformidlingen, [2008]. S. 121–140 – (Det juridiske fakultets skriftserie ; nr 114)

1 Illustrasjonen er hentet fra Øyvind Hallsteinsen [et al.], Innføring i datakommunikasjon, Oslo 2005, s. 53. Fremstillingen i artikkelens kapittel 2 er basert på samme bok, i tillegg til samtaler med overingeniør ved UiOs IT-avdeling Ingar Vindenes, systemutvikler ved Bekk Consulting AS Vidar Kongsli og programmerer ved Arm Norway AS Mikael Levernes Valen-Senstad.



Transporten av en e-post kan sammenlignes med tradisjonell postforsendelse. E-postklienten, for eksempel Outlook, Eudora, eller Hotmail, pakker e-posten inn i en konvolutt («envelope») med informasjon om hvem meldingen er fra og hvor den skal til, og sender brevet til den lokale e-posttjeneren. E-posttjeneren har to oppgaver: Den formidler e-post for sine klienter og administrerer lokale postkasser. E-posttjeneren ser på konvoluttinformasjonen og sender posten til mottakerens e-posttjener. Her tas konvolutten av og kun selve brevet legges i mottakerens postkasse.

Informasjonen på konvolutten lages i utgangspunktet automatisk av e-postklienten, men den kan også enkelt lages av avsenderen. I og med at e-postleseren ikke ser på selve brevet, men kun forholder seg til konvolutten, er det fullt mulig at angitt mottager i brevet ikke samsvarer med angitt mottager på konvolutten. Dette vil ikke mottakeren se uten å kontrollere konvolutten. Her er det altså muligheter for feil og manipulasjon, spesielt fra avsenders side.

Fordi en e-post kun er en tekstfil, er det enkelt å endre den både før, under og etter transporten til mottaker. Dette gjelder også konvoluttinformasjonen. Forsendelse av en usikret e-post kan sammenlignes med å sende et postkort skrevet med blyant. Innholdet er tilgjengelig for samtlige postmedarbeidere og det er enkelt å viske ut noe av informasjonen og eventuelt erstatte det med noe annet.

Det finnes to måter å sikre autentisiteten av en e-post; gjennom kryptering og ved å påføre e-posten en elektronisk signatur. Begge måter krever at

mottaker og avsender av e-posten har en nøkkel eller en form for sertifikat.[2] Kryptering innebærer konfidensialitet. Kun mottaker har nøkkelen til å «låse opp» e-posten og lese den. En e-post med e-signatur er derimot usikret på den måten at alle ledd under transporten kan lese informasjonen, men ikke foreta endringer, verken av konvoluttinformasjonen eller selve innholdet. Analogien kan være et postkort skrevet med penn. E-signaturen sikrer at det ikke skjer endringer av e-posten under transporten og avsenders identitet sikres.

Verken kryptering eller e-signatur brukes i særlig utstrekning i dag. Dette gjelder også e-post som inneholder sensitiv informasjon.

3 E-post som bevis

E-post er en kommunikasjonsform som i løpet av få år har fått stor samfunnsmessig betydning i Norge. Dette får også innvirkning på bevis i rettstvister.[3] Første gang bruk av e-post dukker opp som et bevisspørsmål i en publisert rettsavgjørelse var i 1997.[4] Retten uttalte om det tekniske fenomenet: «E-post, der E står for elektronisk, er en melding som sendes fra avsenderens datamaskin til mottakerens. […] Sendinger av E-post har klare likhetstrekk med tradisjonell sending av brev, telegram og for den saks skyld den mer moderne kommunikasjonsform telefaks.» Uttalelsene gir et bilde av e-post som vi i dag, 10 år senere, ser på som historiske. Selv om ikke alle har internettoppkobling hjemme, har de aller fleste tilgang til PC og internett på arbeidsplass, skole, bibliotek eller lignende. Bruk av e-post er blitt en naturlig og integrert del av hverdagen på de fleste arbeidsplasser.[5]

E-post har mange likhetstrekk med andre skriftbaserte bevis. På samme måte som det meste av skriftlig kommunikasjon i våre dager, produseres e-post ved bruk av datamaskin. Det er imidlertid flere forhold som særpreger e-post, både når det gjelder tilblivelse, forsendelse og etterfølgende lagring. Et typisk trekk er at e-post i utgangspunktet kun håndteres elektronisk. Brev og kontrakter som er beregnet på å bli håndtert i papirformat, skrives ut når teksten eller innholdet er ferdig bearbeidet, og i mange tilfeller signeres også dokumentet for hånd. Overføringen til papirformat har viktige implikasjoner.

2 Ot.prp. nr. 82 (1999–2000), Om lov om elektronisk signatur, s. 11

3 St.meld. nr. 17 (2006–2007) Eit informasjonssamfunn for alle, s. 14–15. Dens grunnleggende funksjoner ble utviklet av Ray Tomlinson, en programmerer for det amerikanske IT-selskapet BBN, i juli 1970. Manuel Castells, The internet galaxy. Reflections on the internet, business, and society, Oxford 2001, s. 18.

4 Avgjørelse i Borgarting lagmannsrett 26. september 1997, inntatt i RG 1998 s. 1155. Med «publisert» menes avgjørelser som er tilgjengelig på Lovdata.

5 St.meld. nr. 17 (2006–2007), s. 15

Ved å skrive ut et dokument, og eventuelt datere og signere det, får dokumentet en bevismessig identitet. Derved låses i praksis redigeringsmuligheten for dokumentet. E-post har ikke samme integritet som bevis. E-post trenger ikke skrives ut for å sendes til mottager, og oftest tar verken avsender eller mottager papirutskrift av meldingen. Hvis det senere oppstår en tvist, og det er av bevismessig interesse å påberope innholdet av elektronisk kommunikasjon, presenteres beviset normalt ved at man i ettertid tar utskrift og fremlegger denne. Man har imidlertid begrenset sikkerhet for at slike uskrifter av e-post i alle henseender gir korrekt informasjon. Papirutskriften som presentasjonsform avskjærer i seg selv muligheten for å sjekke meldingens konvoluttinformasjon for å klarlegge mulig tvil om autentisitet og innhold.

E-post kan redigeres uten at verken skjermbildet eller papirutskriften normalt gir leseren informasjon om eventuelle tidligere versjoner. Det fremgår ikke hva som eventuelt er endret eller når dette er skjedd, heller ikke hvem som kan ha foretatt endringer. E-post er derfor ømfintlig for manipulasjoner og egnet til å forlede den som skal vurdere bevisverdien av en utskrift i ettertid. Det er en smal sak å produsere en utskrift av en e-post som uriktig hevdes å være sendt eller mottatt, men papirutskriften gir ingen veiledning for å vurdere dette. Ved bruk av e-post skjer hyppig også innholdsmessige endringer uten at det er tilsiktet å forlede noen, f.eks. ved at man i en lengre e-postveksling ved bruk av svar- eller videresendingsfunksjonen av praktiske grunner velger å slette deler av innholdet som oppfattes som forstyrrende eller unødvendig haleheng. Eller det kan være at man velger å redigere innholdet av informasjon som videresendes for å rette feil, eller for å markere et annet syn eller meningsinnhold for mottakeren. En utskrift vil objektivt sett dermed være å fremvise et manipulert bilde av hva som var meldingens opprinnelige utforming.

En annen sentral egenskap som knytter seg til e-post, er hurtigheten. Mens tradisjonell postgang kan ta dager, er e-post formidlet på sekunder. Dette gjør at e-posten kan konkurrere med telefonkommunikasjon, noe som naturlig vil påvirke stil, form og innhold. E-posten får en langt mer muntlig og uhøytidelig form enn vanlig skriftlig kommunikasjon per brev. En kommunikasjonsform som i enda større grad kommer i gråsonen mellom skriftlig og muntlig kommunikasjon er chatting, en slektning av e-posten. Generelt kan man si at e-post har påvirket den alminnelige kommunikasjon ved etablering av et nytt nivå mellom den mer formelle og presise skriftlige form og den uformelle, direkte og løse stil som normalt kjennetegner muntlig tale. Dette får nødvendigvis betydning ved en senere bevisvurdering. En kontant og kanskje sleivete e-postmelding – selv om den er skriftlig – bør ikke tolkes på samme måte som et formelt brev, hvor ordvalg og stil gjerne blir annerledes.

Nettopp fordi e-post er hurtig og effektiv, er den blitt en teknologisk suksess. Den omfattende bruken innebærer en enorm skriftlig tekstproduksjon uten sidestykke i historien. En konsekvens av dette er at den faktiske forekomst og tilgang til skriftlig dokumentasjon på historisk kommunikasjon blir overveldende. Mens man tidligere kommuniserte muntlig, i telefon og i møter, sender man i dag gjerne en e-post. Det innebærer at man for eksempel i tvister om kompliserte løpende forretningsforhold ofte kan fremlegge store mengder av utskrifter av partenes kommunikasjon fra time til time. På den måten er det mulig å bevismessig gjenskape en langvarig prosess på en helt annen og sikrere måte, sammenlignet med tidligere tider hvor man i større grad var henvist til vitneforklaringer basert på mangelfull eller selektiv hukommelse. Konsekvensen av den store forekomst av e-post som bevis kan være praktiske utfordringer knyttet til tilgang, avgrensning og presentasjon av et slikt materiale for retten.

E-post brukes både til privat og jobbrelatert kommunikasjon. I datamaskinen lagres e-post i utgangspunktet kronologisk, noe som medfører at private og jobbrelaterte meldinger står side om side. Ved innsyn i en persons e-postkonto, f.eks. i forbindelse med bevissikring, vil man dermed få tilgang til langt mer informasjon enn det man i praksis er ute etter. Til forskjell fra et papirbasert arkiv, hvor man finner et dokument uten å åpne alle skuffer og saksmapper, kan man ikke hente ut en e-postmelding fra en e-postkonto uten samtidig å skaffe seg tilgang til også meldinger som kan være av f.eks. privat karakter. Det skaper personvernmessige utfordringer. Organiseringen av e-post på en datamaskin gir derfor opphav til praktiske prosessuelle spørsmål. Å gi en arbeidsgiver eller motpart alminnelig tilgang til en persons e-post, ville i praksis være alt for vidtrekkende. Tilgangen til e-post har derfor vært et tilbakevendende spørsmål i arbeidsrettslige konflikter. Jeg kommer inn på dette under pkt. 8.

4 Bevisreglene i tvisteloven

Tvistemålsloven inneholdt ingen særbestemmelser om håndtering av e-post, og overgangen til den nye tvisteloven innebærer bare en liten endring i så måte. Den eneste bestemmelsen i tvisteloven som nevner elektronisk lagret materiale, er § 26–1 som slår fast at dette er et realbevis. Utover dette, inneholder loven ingen særregler for verken elektroniske bevis generelt eller e-post spesielt, og vi er derfor henvist til de alminnelige bevisreglene.

Norsk sivilprosess er basert på disposisjonsprinsippet. Det innebærer at partene selv bestemmer hvilke krav retten skal avgjøre, jf. § 11–2 (1). Partene er gjennom forhandlingsprinsippet pålagt å sørge for bevisføringen, jf. § 11–2

(2), og i utgangspunktet kan de, etter prinsippet om fri bevisførsel, føre de bevis de ønsker, jf. § 21–3. Bevisførselen utgjør det faktiske avgjørelsesgrunnlaget og partene har plikt til å sørge for at saken blir riktig og fullstendig opplyst. «En part skal også opplyse om viktige bevis som parten ikke har hånd om, og som parten ikke har grunn til å regne med at den annen part er kjent med. Dette gjelder uansett om beviset er til støtte for parten selv eller den annen part.», jf. § 21–4 (2). Dette understøttes i den allmenne forklarings- og bevisplikten i § 21–5: «Enhver plikter å gi forklaring om faktiske forhold og gi tilgang til gjenstander mv. som kan utgjøre bevis i en rettssak […]».

Loven tegner som et utgangspunkt et bilde av en ideell verden der partene hjelper hverandre til å finne bevis som fører til at dommeren får et godt balansert bilde av saken, og dermed har det beste utgangspunkt for å avsi en materielt riktig dom. Virkeligheten er langt mer nyansert. Partene i en sivil sak kan ha interessemotsetninger som medfører at de gjør hva de kan for å vanskeliggjøre bevisførselen. Tvisteloven har likevel virkemidler som i rimelig grad sikrer at dommeren får et riktig faktisk grunnlag for sin avgjørelse.

5 Bevistilgang[6]

5.1 Plikten til å stille realbevis til rådighet

Etter tvl. § 26–5 (1) har partene plikt til etter begjæring å stille til rådighet «gjenstander», herunder e-post, som vedkommende «har hånd om eller kan skaffe til veie». Et særtrekk ved denne formen for bevisinnhenting er at parten selv kan håndtere beviset før det overlates til motparten. Dette har både positive og negative sider. En positiv effekt er at mange personvernsmessige spørsmål kan ryddes av veien. Partene kan selv sile vekk e-post med privat eller sensitiv informasjon, og behovet for å engasjere tredjemenn til å håndtere bevisene reduseres. Utfordringen er at partenes håndtering av e-postene er basert på et tillitsforhold som lett kan misbrukes, og eventuelt misbruk kan være vanskelig å oppdage. Slik sett er det utilfredsstillende å sette motparten selv til å utføre arbeidet med å sortere bevisene.

Plikten i § 26–5 (1) omfatter i utgangspunktet alle gjenstander som etter § 26–1 «inneholder informasjon som kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken». Dette gjelder imidlertid med visse begrensninger.

6 For en bredere fremstilling av bevistilgang til elektronisk materiale i sivile saker, se Erik Monsen, Bevistilgang til elektronisk material, Tidsskrift for Forretningsjus 2007 nr. 3, s. 194–235.

Anfører motparten at beviset er omfattet av et bevisforbud eller bevisfritak etter tvisteloven kapittel 22, kan ikke beviset legges frem, med mindre retten «i kraft av særlig lovbestemmelse kan bestemme at beviset likevel skal føres», jf. § 26–7 (2). Bestemmelsen understreker bare den alminnelige reglen i § 21–3 (1) om muligheten til å få avskåret bevis med en anførsel om bevisforbud eller bevisfritak og innebærer således ikke noe nytt. Rettens mulighet til å avgjøre at et bevis likevel skal kunne kreves fremlagt, ville uansett vært tilstede etter de enkelte bestemmelsene i kapittel 22, jf. pkt. 7 om bevisavskjæring nedenfor.

Også de alminnelige reglene om unntak fra retten til å føre bevis i §§ 21–7 og 21–8 får anvendelse på begjæring om bevistilgang. Lovgiver har likevel valgt å regulere også dette eksplisitt i kapittel 26. Etter tvl. § 26–5 (3) kan retten nekte tilgang til et bevis dersom hensynet til proporsjonalitet taler mot det, jf. § 21–8. Videre kan retten, i vurderingen av om en part skal gis tilgang til et bevis, etter § 26–7 (1) «kreve gjenstanden fremlagt til avgjørelse av om den utgjør et bevis», jf. § 21–7. Betydningen av disse reglene i forhold til e-post som bevis behandles også under pkt. 7 nedenfor.

5.2 Spesifikasjonskravet

For at en part skal kunne pålegges å gi tilgang til bevis, må motparten, etter tvl. § 26–6, spesifisere hvilke bevis han eller hun ønsker tilgang til. Dette spesifikasjonskravet er en videreføring av kravet til individualisering som tidligere var forankret i tvml. § 253. Dersom spesifikasjonen ikke er tilstrekkelig, vil retten kunne avslå begjæringen, fordi det i praksis da blir uklart hva som skulle omfattes. Beviset må derfor individualiseres og spesifiseres, slik at det er klart hvilke bevis ønskes adgang til.[7] Hva dette klarhetskravet innebærer, er utviklet gjennom rettspraksis. Svært få av disse avgjørelsene dreier seg imidlertid om tilgang til e-post, men det kan likevel trekkes slutninger om hvordan gjeldende rett er i forhold til denne typen bevis. Kjennelsen inntatt i Rt. 2007 s. 920 gjaldt blant annet tilgang til kontoutskrift for to bestemte bankkonti, for den ene kontoen «i perioden fra og med 1993 til kontoens avslutning, formodentlig i 1999» og for den andre «fra og med 1999 og til kontoens avslutning». Høyesteretts kjæremålsutvalg uttalte at «Kontoen er dessuten individualisert slik at spesifikasjonskravet klart er oppfylt».[8]

En bankutskrift gir oversikt over pengestrømmen, men ikke bakgrunnen for de enkelte transaksjoner. Full tilgang til en samling e-post gir tilgang både

7 Ot.prp. nr. 51 (2004–2005), Om lov om mekling og rettergang i sivile tvister (tvisteloven), s. 204 og s. 467

8 Rt. 2007 s. 920, 46. avsnitt.

til konvoluttinformasjonen, i tillegg til innholdet i meldingene. Sammenlignet med bankutskrifter, må det antas at en begjæring om tilgang til e-post må kreve ytterligere spesifisering. I saken inntatt i Rt. 2004 s. 1467 ble det begjært tilgang til «all e-post korrespondanse mellom henholdsvis Steinar Lund i Diesel Power AS og Braathe Gruppens Fredrik Haugen og all e-post korrespondanse mellom Steinar Lund i Diesel Power AS og Braathe Gruppens Sven R. Nilsen for perioden 19. juli 2002 til 11. desember 2002 som angår ClientPartners overtakelse av Intellinets konkursbo, herunder informasjon om konsekvenser av overtakelsen for løpende kontraktsforhold om overføring av avtaler, samt korrespondanse som angår ClientPartners varsling av flytting», i tillegg til «e-post sendt blant annet til Diesel Power fra ClientPartner 19. juli 2002, 21. juli 2002 og 22. juli 2002».[9] Denne spesifikasjonen ble ansett tilstrekkelig klar, jf. kjennelsens 23. avsnitt. Hvorvidt klarhetskravet i tvl. § 26–6 (1) er oppfylt ved begjæring om tilgang til e-post beror på en skjønnsmessig helhetsvurdering. Det sentrale er om informasjonen er angitt så presist som praktisk mulig, f.eks. med angivelse av mottaker, avsender, tidsrom for forsendelsen(e) og tema for meldingens innhold. Spesifikasjonen skal gjøre det praktisk mulig for rette vedkommende å identifisere og fremskaffe materialet uten vesentlig tvil om hva fremleggelseskravet faktisk omfatter.

I tillegg til at spesifikasjonen må være tilstrekkelig klar, må det eksplisitt eller implisitt følge en pretensjon om at bevisene faktisk eksisterer og vil utgjøre relevante bevis. En part kan ikke be om en e-post som ikke vil utgjøre noe bevis i saken eller anmode om tilgang til noe som vedkommende bare spekulerer på om eksisterer. Dette understrekes i Rt. 2007 s. 920 i 39. og 49. avsnitt, Rt. 2004 s. 351 i 22. avsnitt og i Rt. 1998 s. 484 på side 486.

I tvl. § 26–6 (2) åpnes det for å lempe på spesifikasjonskravet. For at unntaksregelen skal komme til anvendelse, må kravet til spesifikasjon være «uforholdsmessig vanskelig å etterkomme», og det må være «en nærliggende mulighet» for at kravet kan gi tilgang til bevis. Begrunnelsen for denne unntaksregelen er hensynet til å få saken forsvarlig opplyst.[10] Forarbeidene gir ingen utfyllende forklaring på eller eksemplifisering av hvilke forhold som tilfredsstiller kravet til at spesifikasjon er «uforholdsmessig vanskelig å etterkomme», men åpner for en vid skjønnsmyndighet fra rettens side.[11] Det legges videre vekt på at en proporsjonalitetsvurdering skal stå sentralt ved vurderingen av § 26–6 (2).[12] Konsekvensen synes å bli en utvanning både av spesifikasjonskravet

9 Rt. 2004 s. 1467, 7. avsnitt.
10 NOU 2001:32, Rett på sak. Lov om tvisteløsning (tvisteloven), s. 980
11 Ot.prp. nr. 51 (2004–2005), s. 468
12 NOU 2001:32, s. 980

i § 26–6 (1) og av spesifikasjonskravet generelt, i og med at en proporsjonalitetsvurdering allerede står sentralt i § 26–5 (3). «Det man står igjen med, er et spesifikasjonskrav med begrenset praktisk interesse. Angående omfanget av edisjonsplikten er det først og fremst forholdsmessighetsvurderingen som vil ha praktisk betydning, og da ikke bare som en begrensning, men også som et argument for bevistilgang i saker av stor betydning».[13]

Muligheten for lemping av spesifikasjonskravet kan få betydning for tilgang til e-post. E-post er et bevismiddel hvor det nettopp kan være vanskelig å oppfylle spesifikasjonskravet når man ikke kjenner detaljer, f.eks. hvilke personer i en bedrift som har kommunisert om et tema, til hvilke tidspunkter osv., selv om det fremstår overveiende sannsynlig at relevant bevis befinner seg på bedriftens e-postserver. Konsekvensen kan bli at retten lemper på kravene til spesifikasjon, med tilsvarende risiko for at motparten får innsyn utover det som vedkommer saken.

5.3 Partens tilgang til beviset

I tillegg til å kreve at det spesifiseres hvilke bevis en ønsker tilgang til, oppstiller tvl. § 26–5 (1) et krav om at motparten «har hånd om eller kan skaffe til veie» beviset. Dette er en videreføring av besittelseskravet i tvml. §§ 250 og 251. For at motparten skal kunne pålegges å gi tilgang e-postene, må han eller hun ha tilgang til dem. Dette vilkåret kan være av særlig interesse der e-postene er flyttet over på et annet medium eller er slettet, slik at det kreves datakyndig personell for å tilgjengeliggjøre dem.

Retten kan etter tvl. § 26–5 (3) nekte bevistilgang dersom den begjærende part har «tilnærmet samme mulighet for tilgang». Dette er basert på en proporsjonalitetsvurdering der en part som like lett kan fremskaffe beviset, ikke skal kunne belaste motparten med denne praktiske byrden.[14] Vi finner et eksempel på en slik proporsjonalitetsvurdering i Rt. 2004 s. 1467. Her var sikkerhetskopiene av Diesel Powers e-postkorrespondanse kopiert over på en CD, og den lot seg ikke åpne uten eksperthjelp. Høyesteretts kjæremålsutvalg mente likevel at e-postene var i Diesel Powers besittelse og at de selv hadde ansvar for å tilveiebringe eksperthjelpen, dette til tross for at motparten, ClientPartner, hadde tilgang til den samme e-postkorrespondansen. ClientPartner fikk medhold av Høyesteretts kjæremålsutvalg i at formålet med å begjære tilgang ikke var å belaste Diesel Powers med arbeidet med å åpne

13 Monsen (2007), s. 218
14 NOU 2001:32, s. 980

CD-en, men å få bekreftet mottagelsen av e-postene. Dette kunne de ikke få ved å legge frem sine egne kopier av e-postene.

5.4 Gjennomføring av edisjonsplikten

Den vanligste formen for gjennomføring av edisjonsplikten, er å stille e-postene til rådighet for motparten, jf. tvl. § 26–5 (1). Det er ikke eksplisitt regulert, verken i § 26–5 (1) eller i § 26–7 (3), i hvilken form e-postene skal stilles til rådighet. Etter § 26–7 (3) overlates dette til retten å avgjøre. Lovkommentaren nevner både papirutskrifter og elektronisk kopi.[15] En tilgang til kun papirutskrifter vil kunne begrense informasjonsverdien av bevisene, jf. pkt. 8 nedenfor. Den praktiske fremgangsmåten i dag er imidlertid å fremlegge papirutskrifter av de fremprovoserte e-postene med prosesskrift. Det er lite sannsynlig at denne fremgangsmåten endres i praksis, med mindre lovforslag og tekniske løsninger legger opp til en annen praksis. Etter omstendighetene kan det være et alternativ å formidle en harddisk til motparten for gjennomgang av et materiale, slik at motparten selv kan velge hva som bør fremlegges i form av utskrift.

Loven legger i § 26–5 (2) opp til at parten også kan bli pålagt å svare på spørsmål om bevisgjenstander og «foreta nødvendige undersøkelser i den forbindelse». Denne bestemmelsen kan, i likhet med § 26–6 (2), sees på som en utvanning av spesifikasjonskravet. Dersom en part ikke er i stand til å spesifisere tilstrekkelig hvilke e-post man ønsker tilgang til, kan motparten likevel pålegges å utferdige lister over e-post eller svare på spørsmål som så i neste omgang kan gi parten tilstrekkelig informasjon til å oppfylle spesifikasjonskravet. Forarbeidene ser på denne bestemmelsen som en effektivisering av den allmenne sannhets- og opplysningsplikten, og det uttales at bestemmelsen er utviklet etter et ønske om større åpenhet rundt bevismaterialet.[16] Også denne bestemmelsen skal imidlertid balanseres etter et proporsjonalitetsprinsipp. Plikten er begrenset ved at det ikke skal være et misforhold mellom ulemper og omkostninger ved å besvare spørsmålene og foreta de nødvendige undersøkelser, og den mulige verdien av tvisten. Monsen skisserer eksempler på spørsmål partene kan stille for å få tilstrekkelig informasjon til å kunne be om spesifikke e-poster. Selv om spørsmålene er generelle, er det nærliggende at for eksempel en saksøkt konkurrent vil motsette seg å gi detaljert informasjon om nettverksserveren, hvem av de ansatte som benytter seg av hjemme-pc, rutiner

15 Tore Schei, Arnfinn Bårdsen, Dag Bugge Nordén, Christian H. P. Reusch og Toril M. Øie, Tvisteloven (lov av 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister) Kommentarutgave, Oslo 2007, s. 1224

16 NOU 2001:32, s. 979 og Ot.prp. nr. 51 (2004–2005), s. 467

for lagring, hvilken maskinvare og programvare firmaet benytter, hvordan maskinene er knyttet sammen i nettverk, samt fil- og mappestruktur for lagret informasjon.[17] Dette er informasjon som kan være både sensitiv i forhold til konkurranse og sikkerhet.

Etter tvl. § 26–5 (2) annet punktum kan en part også pålegges å utferdige «sammenstillinger, utdrag eller annen bearbeiding av opplysninger», typisk i form av lister over e-post. Dette er en nyvinning i tvisteloven, og i forarbeidene anføres det at regelen «passer bedre i et samfunn hvor viktig informasjon i stadig høyere grad lagres elektronisk, og hvor det i eksisterende programvarer ofte vil ligge vidtgående muligheter til å få ut bearbeidelser og sammenstillinger mv. som kan være av vesentlig bevisverdi i saken».[18] Også her vil proporsjonalitetsprinsippet legge en begrensning for hva som kan kreves av arbeid for å utarbeide oversiktene.

Selv om det kan virke som om Tvistemålsutvalget i utgangspunktet har tenkt på tallmessige fremstillinger, kan løsningen kan være praktisk også med sikte på e-post. Ved å begrense innsynet til en oversikt over hvem e-postene er sendt til og fra og temaet for meldingene, kan dette begrense noen personvernsmessige problemstillinger. Dessuten har de fleste e-postklienter søkemuligheter for informasjonen i e-postens meldingshode, slik at relevant e-post kan identifiseres uten bruk av store ressurser. Faren er at motparten, ved at retten lemper på spesifikasjonskravet, får oversikt over e-postkorrespondanse som ikke vedkommer saken og som kan være av sensitiv karakter. På den annen side er det parten selv som skal utferdige oversikten. Dette forebygger risikoen for utilsiktet innsyn i taushetsbelagt materiale.

6 Bevissikring

6.1 Vilkår for bevissikring

Tvl. § 26–5 regulerer at motparten har plikt til å stille til rådighet «gjenstander», herunder e-post, som vedkommende «har hånd om eller kan skaffe til veie». Likevel kan være behov for å sikre bevis i forkant av saken etter tvisteloven kapittel 28.[19] Bevissikring etter tvl. § 28–2 kan begjæres dersom det er «en nærliggende risiko for at beviset vil gå tapt eller bli vesentlig svekket, eller av andre

17 Monsen (2007), s. 214
18 NOU 2001:32, s. 979
19 Av hensyn til artikkelens omfang behandler jeg ikke bevisopptak i rettssak, tvistelovens kapittel 27, i denne artikkelen.

grunner er særlig viktig å få tilgang til beviset før sak er reist». Bestemmelsen omtaler to alternative vilkår som begge kvalifiserer til bevissikring.

Bestemmelsens første alternativ er iht. forarbeidene knyttet til situasjoner der et vitneavhør av forskjellige grunner må avholdes i forkant av hovedforhandling og situasjoner der realbevis vil «råtne eller endre egenskaper over tid».[20] Bestemmelsen viderefører på dette punktet «langt på vei» tvml. § 267 (1), men har fått en mer moderne språkdrakt.[21] Forarbeidene nevner ikke e-post i denne sammenheng, men man kan tenke seg situasjoner hvor e-post kan stå i fare for å bli slettet rutinemessig. Selv om det oftest er mulig å spore opp slettet e-post, er dette mer ressurskrevende enn å få tilgang til relevant e-post fra innboksen, og hensynet til proporsjonalitet kan føre til at beviset ellers blir avskåret. Også motpartens kunnskap om en mulig forestående rettstvist vil kunne innebære bevisforspillelsesfare som kan ivaretas av dette alternativet.

Bestemmelsens andre alternativ – «andre grunner» – blir i forarbeidene anført å være aktuell som virkemiddel for å få vurdert en rettslig situasjon. Tanken er at en part med henblikk på en mulig rettstvist, kan få tilgang til bevis fra den potensielle motpart. På den måten skal man kunne unngå å anlegge sak på et uholdbart faktisk grunnlag.[22] I forhold til e-post kan imidlertid slik bevistilgang medføre personvernsmessige problemstillinger. En part kan også tenkes å spekulere i å oppnå slik bevistilgang utenfor rettssak med sikte på å skaffe seg et konkurransemessig fortrinn eller kunnskap om en annens bedriftsinterne forhold – har en part først fått en informasjon, kan den ofte ikke trekkes tilbake. Bestemmelsens vilkår om at tilgangen til beviset må være «særlig viktig» gir imidlertid anvisning om en streng vurderingsnorm for å forhindre slike situasjoner. I tillegg kan den som har begjært bevissikring holdes ansvarlig for skade den aktuelle motparten har lidt, dersom motparten ikke ble varslet før bevissikringen ble holdt og det viser seg at det ikke fantes krav eller rettigheter som bevissikringen skulle tjene til å beskytte, jf. § 28–3 (5).

6.2 Varsling av motparten

Av hensyn til kontradiksjon, skal motparten vanligvis varsles før en bevissikring. Dersom det ikke lar seg gjøre å varsle i tide, skal det oppnevnes en representant for motparten, for at denne skal kunne ivareta motpartens interesser, se § 28–3 (3). I noen tilfeller vil imidlertid grunnlaget for bevissikringen ødelegges dersom motparten får informasjon om en forestående bevissikring.

20 ibid., s. 987
21 ibid., s. 988
22 Schei m.fl. (2007), s. 1247

Retten kan derfor etter tvl. § 28–3 (4) treffe avgjørelse om at bevissikring skal holdes *før* motparten varsles dersom det er «grunn til å frykte at varsel til motparten vil kunne hindre at beviset sikres».

Forarbeidene sier lite om hvilke situasjoner denne bestemmelsen er ment for. Bestemmelsen er foranlediget av «hensynet til å kunne oppfylle Norges forpliktelser i den såkalte TRIPS-avtalen – Trade Related Aspects of Intellectual Property Rights».[23] Av den grunn ble tilsvarende bestemmelse innført i tvml. § 271a, med virkning fra 1. juli 2004. Denne bestemmelsen har i praksis blitt brukt til å sikre elektroniske bevis, herunder e-post. Det finnes foreløpig ingen avgjørelse som spesifikt gjelder bevissikring av e-post, men i den såkalte Normarc-saken, Rt. 2006 s. 626, ble det foretatt speilkopiering av blant annet flere e-postservere. Tvml. § 271a er videreført i tvl. § 28–3 (4)-(6)[24].

E-post kan enkelt slettes eller manipuleres, og det kan være umulig eller ressurskrevende i etterkant å gjenopprette en tidligere bevissituasjon. Dersom en part får anmodning fra en potensiell motpart om innsyn i e-postkorrespondanse, kan dette nærmest være en oppfordring til slette eller på annen måte fjerne eller redigere informasjon som man ikke ønsker at andre får tak i. For e-post vil det nesten alltid kunne anføres en frykt for «at motparten vil kunne hindre at beviset sikres». Det er likevel ikke noen nødvendig sammenheng mellom denne frykt og muligheten for å få sikret e-post i forkant av en eventuell rettstvist. I forarbeidene blir § 28–3 (4) presentert som en unntaksbestemmelse, og i kommentarutgaven til loven manes det til varsomhet mot i praksis å utvide anvendelsesområdet til bestemmelsen.[25]

6.3 Spesifikasjonskravet

Sikring etter § 28–3 (4) stiller krav til en viss spesifikasjon av de bevisene som ønskes sikret. I Rt. 2006 s. 626, 35. avsnitt, slår Høyesteretts kjæremålsutvalg fast at det ikke kan stilles like strenge krav til spesifikasjon i forbindelse med bevissikring som ved bevistilgang. I lovkommentaren anføres det imidlertid at dette ikke kan gjelde etter tvisteloven. I og med at kravet til spesifikasjon ved bevistilgang nå kan lempes etter § 26–6 (2), «kan det ikke lenger være grunn til å operere med et mildere spesifikasjonskrav for bevissikring etter § 28–3 fjerde ledd enn for andre begjæringer om bevistilgang».[26]

23 NOU 2001:32, s. 989–990
24 Ot.prp. nr. 51 (2004–2005), s. 471
25 NOU 2001:32, s. 989 og Schei m.fl. (2007), s. 1254.
26 Schei m.fl. (2007), s. 1254

Lempingsmuligheten i § 26–6 (2) er imidlertid neppe et tilstrekkelig argument for å likestille spesifikasjonskravet for bevistilgang i rettssak og bevissikring utenfor rettssak. Ved begjæring om bevistilgang har man andre muligheter, dersom man ikke evner å oppfylle spesifikasjonskravet, blant annet å stille motparten spørsmål og be om sammenstillinger eller oversikter over materialet, jf. § 26–5 (2). Denne muligheten har man av naturlige grunner ikke etter § 28–3 (4). Kommunikasjon med den aktuelle motparten om dette vil lett kunne føre til at formålet med bevissikring ikke oppnås. Dette taler for at spesifikasjonskravet ved bevissikring fremdeles bør ligge lavere enn kravet ved bevistilgang. Motpartens rettssikkerhet ivaretas blant annet ved adgangen til å be om etterfølgende rettsmøte, som kan innlede prosess for nærmere gjennomgang og sortering av materialet før det stilles til disposisjon for saksøker. Loven gir imidlertid ingen nærmere anvisning på hvordan denne prosess skal gjennomføres, med sikte på å sortere ut materiale som må ansees irrelevant eller taushetsbelagt. I praksis vil det bli behov for sakkyndig bistand, jf. Rt. 2006 s. 626, 37. avsnitt, og i tvilstilfelle må retten ta stilling til den enkelte e-post som partene måtte være uenige om skal inngå i bevismaterialet.

7 Bevisavskjæring

7.1 Bevisavskjæring etter de alminnelige bevisreglene

Tvl. § 21–3 (1) hjemler unntak fra partenes rett til å føre bevis gjennom å vise til §§ 21–7, 21–8 og bestemmelsene i kapittel 22 om bevisforbud og bevisfritak, samt en generell henvisning til bevisreglene.

Tvl. § 21–7 oppstiller alminnelige begrensninger, hvor særlig § 21–7 (2) c) har praktisk betydning i relasjon til e-post. Retten har mulighet til å nekte bevis ført hvis den «finner det nødvendig å føre beviset på annen måte». Forarbeidene nevner «hearsay evidence» som eksempel, dvs. vitneforklaringer fra tredjepersoner om hva noen andre har sett eller hørt.[27] I slike tilfeller ønsker retten normalt heller å høre forklaringen fra vedkommende selv, dersom dette lar seg gjøre. Lovkommentaren nevner også situasjoner der man avskjærer en kopi når det er av betydning at originalen legges frem og dette er mulig.[28] I forhold til e-post må konsekvensen bli at retten kan kreve e-postbeviset ført i elektronisk versjon, istedenfor i form av papirutskrift. Dette

27 NOU 2001:32, s. 949
28 Schei m.fl. (2007), s. 1016

vil nok normalt være upraktisk, men § 21–7 kan være hjemmel hvis det skulle være av betydning for retten å granske selve lagringsmediet.

Det uttales i forarbeidene at kravet etter § 21–7 må avveies i forhold til prinsippet om proporsjonalitet inntatt i § 21–8, se nedenfor.[29] Avhengig av hvor strengt dette forstås, kan proporsjonalitetsprinsippet være en begrensende faktor for utøvelsen av § 21–7 (2) c).

Tvl. § 21–8 slår fast prinsippet om proporsjonalitet, et prinsipp som gjennomsyrer tvisteloven. Prinsippet kan ledes ut av lovens formålsparagraf, § 1–1 (2), fjerde strekpunkt, men i tillegg er det nedfelt i flere bestemmelser, herunder §§ 21–8 og 26–5 (3). Prinsippet innebærer et krav til forholdmessighet mellom bevisføringens omfang og sakens betydning. I vurderingen av hva som skal regnes som sakens betydning, vil tvistegjenstandens størrelse være et utgangspunkt, men også andre momenter som ideelle interesser og behovet for rettsavklaring kan tillegges vekt.[30]

Den alminnelige bestemmelsen om proporsjonalitet i tvl. § 21–8 viderefører tvml. § 189 (1) nr. 6, men tvistelovens bestemmelse favner langt videre.[31] Dette gjelder både saklig og prosessuelt. Tvml. § 189 (1) nr. 6 omfattet kun forklaringer, og det var stilt som vilkår at bevisførselen «vilde medføre et opphold». Tvl. § 21–8 omfatter derimot alle typer bevis, herunder e-post, og bevisførselen kan begrenses ganske dramatisk i mindre saker, så fremt det ikke strider mot ønsket om å komme frem til et materielt riktig resultat. Begrensningen kan, for e-postens vedkommende, gjøres enten ved at beviset helt avskjæres eller ved at partens adgang til å kreve fremlagt metadata av e-post begrenses. Det siste alternativet kan medføre risiko for at retten kan komme til å feilvurdere ektheten eller betydningen av e-postbevis.

7.2 Bevisavskjæring etter tvl. § 22–3

I forhold til bevismiddelet e-post er det særlig to forbudsbestemmelser i kapittel 22 som kan by på utfordringer; nemlig § 22–3 og § 22–7.

Tvl. § 22–3 oppstiller bevisforbud mot opplysninger undergitt lovbestemt taushetsplikt. Første og andre ledd tilsvarer tvml. § 204 nr. 2 første ledd, og viderefører tidligere gjeldende rett.[32] Det er likevel gjort noen endringer. Av betydning er særlig at ordlyden er endret fra å kun gjelde vitneforklaringer, til å omfatte alle typer bevis, inkludert bl.a. e-post. Endringen gjenspeiles også

29 NOU 2001:32, s. 949
30 Schei m.fl. (2007), s. 1019
31 Ot.prp. nr. 51 (2004–2005), s. 455
32 ibid., s. 457

ved at bestemmelsen er flyttet fra tvistemålslovens kapittel om «Vidner og vidneførsel» til tvistelovens kapittel 22 om bevisforbud og bevisfritak som en generell bestemmelse. Det finnes foreløpig ikke publisert rettspraksis der e-post er avskåret med hjemmel i bestemmelsen om taushetsplikt.

En aktuell problemstilling gjelder saker der det er lagret e-post hos for eksempel en tilbyder av en elektronisk kommunikasjonstjeneste som motparten ønsker å bruke som bevis. Tvl. § 22–3 (1) etablerer bevisforbud for forhold undergitt lovbestemt taushetsplikt når opplysningene kommer som følge av «tjeneste eller arbeid for stat eller kommune, […] postoperatør, tilbyder eller installatør av elektronisk kommunikasjonsnett eller -tjeneste». Tilbyder og installatør av elektronisk kommunikasjon har etter lov nr. 83/2003 om elektronisk kommunikasjon (ekomloven) § 2–9 lovbestemt taushetsplikt om innholdet av kommunikasjonen. Etter tredje ledd i § 2–9 er taushetsplikten imidlertid ikke til hinder for at politi, påtalemyndighet og «annen myndighet i medhold av lov» gis abonnementsopplysninger og informasjon om innholdet av elektronisk kommunikasjon. «Det samme gjelder vitnemål for retten». Som eksempel på «annen myndighet» nevner forarbeidene namsmannens rett til innsyn ved behandling av begjæring om utlegg etter tvangsfullbyrdelsesloven § 7–12.[33] Forarbeidene sier imidlertid ingenting om hva som ligger i uttrykket «Det samme gjelder vitnemål for retten». Dersom bestemmelsen skal forstås slik at taushetsplikten opphører idet eier av et elektronisk kommunikasjonsnett blir vitne i en rettssak, vil dette kunne representere et viktig innhugg i taushetsplikten. Det finnes foreløpig bare én avgjørelse om ekomloven § 2–9, inntatt i RG 2006 s. 811, men dette var en straffesak der forholdet til sivilprosessrettslige regler ikke ble behandlet.

Tvl. § 22–3 (2) og (3) oppstiller muligheter for at opplysningene likevel kan legges frem dersom departementet samtykker. Retten har etter tredje ledd mulighet til å overprøve denne beslutningen.

7.3 Bevisavskjæring etter § 22–7

En annen bestemmelse som kan by på utfordringer i forhold til e-post er tvl. § 22–7 om forbud mot bevis fremskaffet på utilbørlig måte. Bestemmelsen er en kodifisering av gjeldende rett utviklet i rettspraksis.[34] Lovgiver har valgt å benytte ordet «utilbørlig» fremfor «ulovlig» for å inkludere de tilfeller som ikke nødvendigvis «rammes av positive lovbestemmelser, men [der] det likevel er klart at fremgangsmåten medfører et slikt inngrep i den personlige

33 Ot.prp. nr. 58 (2002–2003), Om lov om elektronisk kommunikasjon, s. 94
34 Se blant annet Rt. 1991 s. 616, Rt. 1997 s. 795 og Rt. 2001 s. 668.

integritet at den ut fra alminnelige personvernshensyn i utgangspunktet må anses uakseptabel».[35]

Rettspraksis gjelder særlig forholdet mellom arbeidstaker og arbeidsgiver. Det praktiske spørsmål er om arbeidsgivers innsyn i arbeidstakers e-post uten samtykke, kan anses som «utilbørlig». I utilbørlighetsvurderingen angir forarbeidene at det skal legges vekt på om det er «rettssikkerhetshensyn, herunder personvernhensyn,» som tilsier at beviset ikke skal tillates ført.[36] Som motvekt skal det legges vekt på «hensynet til sakens opplysning og den betydning det har å oppnå en materielt riktig avgjørelse».[37] I Rt. 2002 s. 1500 ble nettopp tilgangen til ansattes e-post vurdert. Bedriften mistenkte en ansatt for å planlegge konkurrerende virksomhet, og for å få bekreftet sine mistanker sjekket de hans e-post. Høyesteretts kjæremålsutvalg kom til at de virksomhetsrelaterte e-postene kunne tillates ført som bevis i avskjedssak og at det ikke var utilbørlig at arbeidsgiver hadde lest disse e-postene. Retten viste til den kommende bestemmelsen i tvl. § 22–7 og antydet at den måtte ansees som en kodifisering av «den ulovfestede bevisavskjæringsregel som gjelder i norsk rett». [38]

Utfordringen ved arbeidsgivers tilgang til ansattes e-post er at e-postene kan inneholde opplysninger som er av privat karakter eller taushetsbelagt. Som nevnt under pkt. 2, vil e-post gjerne være sortert kronologisk, uavhengig av om det er tale om privat eller jobbrelatert e-post. Å avgjøre innholdet i en e-post ved kun å forholde seg til emnefeltet, innebærer at man prisgitt avsenders bruk av overskrift. Om den er dekkende, kan bare avgjøres ved lese innholdet. Utilbørlighetsvurderingen i § 22–7 må vurderes bl.a. etter personopplysningsloven § 8 litra f.[39] Bestemmelsen henviser til en balansering av hensyn der arbeidsgivers behov for å ivareta «en berettiget interesse» må veies mot arbeidstakers krav på personvern. I tillegg til Rt. 2002 s. 1500, er RG 1993 s. 77 et eksempel på vurdering av spørsmålet om innsyn i arbeidstakers e-post.

Tvl. § 22–7 er en «kan»-bestemmelse. Det innebærer at retten har rett, men ikke plikt til å avskjære e-post som bevis hvis materialet er fremkommet på utilbørlig vis. I Rt. 2007 s. 920, som hovedsaklig dreide seg om bevistilgang, hadde saksøker benyttet et privat etterforskningsbyrå for å få tilstrekkelige

35 NOU 2001:32, s. 961
36 Ot.prp. nr. 51, s. 459.
37 NOU 2001:32, s. 961
38 Rt. 2002 s. 1500, på side 1502. Spørsmålet om arbeidsgivers adgang til ansattes e-post har senere vært drøftet og utredet i stor bredde, bl.a. i form av utkast til forskrifter fra Datatilsynet, se www.datatilsynet.no. I den juridiske debatt sondres gjennomgående mellom privat og virksomhetsrelatert e-post, en terminologi som ble lagt til grunn i denne Høyesterettskjennelsen.
39 Schei m.fl. (2007), s. 1101

opplysninger til at de kunne provosere frem bevisene. Høyesteretts kjæremålsutvalg konkluderte med at informasjonen var innhentet på utilbørlig vis, men at bevisene likevel ikke skulle avskjæres av «hensynet til sakens opplysning og den betydning det har å oppnå en materielt riktig avgjørelse».[40] I og med at § 22–7 er en såpass skjønnsmessig bestemmelse, vil det være opp til rettspraksis å utforme gjeldende rett.

8 Bevisføring

Elektronisk lagret materiale er som nevnt realbevis, jf. tvl. § 26–1. I reglene om føring av realbevis sondres det mellom dokumentbevis og andre realbevis, se § 26–2 og § 26–3. Verken i NOU 2001: 32 eller i Ot.prp. nr. 51 (2004–2005) sies det imidlertid noe om hva som omfattes av begrepet «dokument».[41]

De fleste dokumenter i dag har en fortid som elektronisk lagret informasjon. Imidlertid er den språklige forståelsen av ordet «dokument» primært knyttet til tekst på papir. Brev, avtaler og lignende blir i stor grad skrevet ut og signert og oppnår dermed dokumentformen. E-post blir sjeldnere håndtert på denne måten. Likheten mellom tradisjonelle dokumenter og e-post er større enn for en del annen elektronisk lagret informasjon, men det kan likevel være store forskjeller. Rettspraksis kan tale for at man skal behandle e-post som et dokumentbevis. Avgjørelsen i Rt. 2004 s. 1467 slår fast i 22. avsnitt at «Det er på det rene – og ikke bestridt – at elektronisk post må anses som skriftlige bevis i forhold til [tvml.] §250». I Borgarting lagmannsretts dom av 20. august 2007[42] blir elektronisk lagrede versjoner av et testament sendt pr e-post ansett som tilstrekkelig bevis for innholdet når originalen var kommet bort. Også Rt. 2003 s. 926 kan tilsi at e-post skal regnes som dokumentbevis, jf. at dette også omfatter videoopptak. Disse rettsavgjørelser gjelder imidlertid spørsmål om bevistilgang og er ikke nødvendigvis avgjørende i forhold til spørsmål om hvordan beviset skal føres.

Ordlyden i tvl. § 26–1 tyder dessuten på at elektronisk lagret materiale ikke omfattes av dokumentbegrepet. I oppregningen av hva som regnes som realbevis vil «fast eiendom, løsøre, dokumenter, elektronisk lagret materiale mv.» etter en naturlig språklig forståelse oppfattes som eksempler på *forskjellige* typer realbevis, og at elektronisk lagret materiale, herunder e-post, følgelig er noe annet enn dokumenter. Dersom dette er lovgivers intensjon, står vi ovenfor et dokumentbegrep som skiller seg tvistemålslovens begrep «skriftlige

40 Rt. 2002 s. 1500, avsnitt 55.
41 NOU 2001:32, s. 977–978 og Ot.prp. nr. 51 (2004–2005), s. 466
42 LB-2006–27667

bevis», jf. tvml. § 250. I og med at de fleste dokumenter i dag som nevnt har en fortid som elektronisk lagret informasjon, vil det generelt være av betydning for bevisføringsreglene å få klargjort begrepet. Verken forarbeidene eller lovkommentaren sier noe om dette, og det må derfor bli opp til rettspraksis å avgjøre hvordan loven skal forstås.

Den praktiske tilnæring til problemstillingen innebærer at man må sondre mellom på den ene side de tilfeller hvor meningsinnholdet og utformingen teksten i en papirutskrift påberopes som bevis og på den annen side de tilfeller hvor den elektroniske lagrede informasjon utgjør og påberopes å ha selvstendig bevismessig betydning. I sistnevnte tilfelle må bevisføringen foregå etter reglene om «andre realbevis», jf. § 26–3, og dommeren må som utgangspunkt selv undersøke beviset. Det er imidlertid naturlig å anta at den tekniske kompetansen hos dommere er varierende, og må man forvente at den praktiske hovedregel blir å undersøke bevisene etter reglene i kapitel 27. Det er også grunn til å anta det i fremtiden, med økt fokus på bevisspørsmål relatert til e-post, oftere blir nødvendig med bruk av sakkyndige i forbindelse med føring av e-post som bevis.

Hvis det derimot er det meningsbærende innhold i teksten i en e-post som påberopes som bevis, vil i praksis bevisføringen foregå etter reglene for føring av dokumentbevis. Bevisføring gjøres da ved at «beviset gjennomgås, og det som er viktig påpekes. Gjennomgåelsen skal ikke være mer omstendelig enn behovet for forsvarlig bevisføring tilsier», jf. tvl. § 26–2. Bestemmelsen gir parten i oppgave å presentere beviset og å forklare for dommeren hvilken betydning det har.

Uttalelsene i forarbeidene og i lovkommentaren tyder på at man i § 26–2 kun har tenkt på den tradisjonelle form for dokumentbevis.[43] Bestemmelsens andre punktum er ment å skulle forhindre omstendelige opplesninger av omfangsrike dokumenter. Dette er en effektivisering i forhold til kravene for bevisføring etter tvistemålsloven, men for e-post treffer bestemmelsen annerledes. I og med at e-post i utgangspunket bare finnes elektronisk lagret, er det som nevnt vanlig at man i dag foretar papirutskrifter av e-post og at disse fremlegges med prosesskrift. En oppfordring i bestemmelsen om å ikke være mer omstendelig «enn behovet for en forsvarlig bevisføring tilsier» kan fungere som en begrensning for bevisførsel om utskriftens bevisverdi i forhold sitt elektroniske opphav og feilkilder i den forbindelse.

43 Schei m.fl. (2007), s. 1203

9 Bevisvurdering

Norsk sivilprosess baseres på en fri bevisvurdering, jf. tvl. § 21–2 (1). Dette innebærer at dommeren skal legge det mest sannsynlige faktum til grunn for avgjørelsen.[44] I vurderingen skal i praksis kun de faktiske forhold som fremkommer under den muntlige forhandlingen tas i betraktning, jf. § 21–2 (2), jf. § 11–1. Det er visse unntak fra regelen om at dommeren bare skal ta i betraktning det partene legger frem, blant annet at dommeren må kunne bygge på sin mer generelle viten og kunnskap, herunder også fagkunnskap, jf. § 21–2 (3). I vurderingen av hva dommeren kan trekke inn av slik kunnskap, skal det vurderes om hensynet til kontradiksjon etter § 11–1 (3) er tilstrekkelig ivaretatt.

Bruk av e-post er i dag en naturlig og integrert del av hverdagen på de fleste arbeidsplasser og grunnleggende kunnskap om e-posten som kommunikasjonsmedium må kunne ansees som generell kunnskap som dommeren uten videre må kunne bygge på.[45] Datakunnskapen vil imidlertid variere fra dommer til dommer.[46] Statistikken viser blant annet generelt at alder er en faktor av betydning.[47] I tvister som innbefatter uvisshet om bevisverdien av e-post kan mangelen på relevant kunnskap føre til at e-postbeviset blir feilbedømt.[48] Manglende datakompetanse kan i verste fall føre til at rettsavgjørelser blir materielt uriktige. I så fall blir dette et spørsmål om rettssikkerhet. Det er heldigvis lite som tyder på at dette er noe problem i dag, men bevisvurderingen kommer sjelden uttrykkelig frem i rettspraksis, og det er dermed vanskelig å vite i hvilken grad feilkildene er hensyntatt.

10 Avslutning

E-posten gjennomsyrer vår hverdag. Den er allerede blitt et sentralt bevismiddel i mange sivile saker. Selv om mesteparten av e-post som påberopes i norske rettssaler utvilsomt gir et dekkende informasjonsbilde av den konkrete virkelighet de er skapt i, er det likevel et prinsipielt problem at e-posten som bevismiddel kan være beheftet med usikkerhet.

Behovet for å innføre elektroniske signaturer ble påpekt allerede på begynnelsen av 1990-tallet, som et viktig redskap for å sikre elektronisk handel.[49]

---

44 NOU 2001:32, pkt. 16.3 og 16.4, på s. 456 flg.
45 St.meld. nr. 17 (2006–2007), s. 15
46 Årsmelding domstolene i Norge 2006, s. 27
47 St.meld. nr. 17 (2006–2007), s. 58–61
48 I artikkel av Ole-Martin Gangnes i Juristkontakt nr. 1/2008, s. 17 flg. påpekes sikkerhetsutfordringene ved bruk av e-post og juristers manglende bevissthet omkring dette.
49 St.meld. nr. 41 (1998–1999), Om elektronisk handel og forretningsdrift, pkt. 5.3 Elektronisk signatur

Handlingsplanen «eNorge 2005» ble lagt frem i mai 2002 og det var da et uttalt mål at «Innen utgangen av 2005 skal forholdene være lagt til rett for allmenn bruk av standardbaserte elektroniske signaturer».[50] I Nasjonal strategi for informasjonssikkerhet utarbeidet i juni 2003 ble dette målet fremhevet som et av fire overordnede mål for informasjonssikkerhet i det norske samfunnet.[51] Ny handlingsplan, «eNorge 2009 – det digitale spranget», ble lagt fram i juni 2005. En sentral målsetning var å etablere en felles offentlig sikkerhetsportal for elektroniske tjenester fra årsskiftet 2005/2006, med tilbud om elektronisk signatur og at alle offentlige brukersteder innen utgangen av 2006 tok i bruk sikkerhetsportalens løsninger.[52] 15. desember 2005 ble sikkerhetsportalen lansert, men allerede i juni 2006 ble det klart at portalen ikke hadde den mengde brukere som regjeringen hadde antatt, og avtalen om sikkerhetsportaltjenester ble derfor avviklet. Etter 2006 har resultatene latt vente på seg. Fornyings- og administrasjonsdepartementet nedsatte en komité sommeren 2006 som fremdeles arbeider med å utarbeide et forslag til strategi for bruk av elektronisk signatur.[53] Før Norges innbyggere forsynes med elektronisk signatur er det urealistisk å tro at det utvikles noen alminnelig praksis for å sikre e-postforsendelsene.

Det er uansett ikke realistisk å vurdere e-post på lik linje med håndsignerte avtaler og brev. Advokater og dommere bør være oppmerksom på de feilkildene som bruk av e-post som bevis kan innebære.

50 eNorge 2005, Nærings- og handelsdepartementet, 2002, s. 15
51 eNorge 2009 – det digitale spranget, Moderniseringsdepartementet, 2005, s. 8
52 B.innst. S. nr. II (2004–2005), Innstilling fra finanskomiteen om Revidert nasjonalbudsjett, pkt. 10.2 og eNorge 2009, s. 26
53 Strategi for eID og e-signatur i offentlig sektor, Fornyings og administrasjonsdepartementet, 2007, høringsversjonen s. 13

HOW CAN ICT REFORM PUBLIC AGENCIES?*

Arild Jansen and Einar Løvdal

Abstract

This study examines the reorganising of the administration of admission to higher education in Norway, which also included the development of a national wide ICT-based case handling system. This reform process was originated by the need to provide politicians with information for control and regulation purposes, that resulted in a centralised management information system. However, it has evolved into a coordinated, but partly distributed decision system that processes most of the applications to higher education in Norway.

Our analysis aims at identifying the driving forces and mechanisms that have motivated this long-term and complex development process. We ask to what extent we may claim that management interests have been the key factor in these reform processes? Or, is it rather advances in new information and communication technologies that have driven the development?

Our conclusions are that neither of these hypotheses can fully explain these processes. It is not disputable that political and central management priorities have been decisive in this reform. At the same time, we cannot neglect the dynamics related to the visions that technological developments have created. Such visions, combined with an enthusiastic development team and supportive managers in the various local institutions have created an environment for innovative technical and administrative solutions.

Introduction

The Norwegian government can celebrate its 50 years anniversary for the use of computers in public administration, as an IBM 360 was put into operation in the spring 1958 for calculating taxes. At the same time, but rather accidentally, the question was raised whether computers will bring about significant organisational change. In their classic 1958 Harvard Business review article, *Management in the 1980s*, Leavitt and Whisler forecast that «IT would replace the traditional pyramidal hierarchy in organisations with a

* This article is based on a paper published on the Nokobit 2008 conference held in Kristiansand, November 17.-19. 2008.

lean structure resembling an hourglass, and productivity would sour through the elimination of most middle managers». Since then, it has been commonplace to assume that ICT has the potential to bring about administrative reform. E.g. Laudon (1974) posed the question of administrative reform specifically with respect to local government. Similarly, Fountain (2002, p 45) says, «Technology is a catalyst for social, economic and political change at the levels of individual, group, organizational and institutions».

Others do, however argue that ICT does not tend to produce reforms (on its own) and that it is not plausible that ICT have been an instrument for administrative reforms (King and Kraemer 1985, George and King 1991). In a more recent paper, Kraemer and King (2008) claim, based on a number of studies of ICT in US government agencies, that ICT rather has been used to reinforce existing administrative and political arrangements.

This paper aims at contributing to this debate in examining to what extent ICT seems to have been an instrument for administrative reform in the Norwegian public sector. The case for this study is the development of NUCAS[1] (The Norwegian Universities and Colleges Admission Service), which coordinates the admission to regular undergraduate studies at all the universities, university colleges, state colleges, and some private colleges in Norway. These development efforts started out as a technical project aiming at providing adequate information about applications for admission, student statistics, etc. to the central government. The results have been, after more than 15 years of development, a web-based, nearly automated admission service, and the building of a new organisation along with comprehensive changes in the legal framework[2].

However, from perspectives of governmental changes, what have been the organisational and institutional implications of this development? Can it be justified to claim that this administrative reform first of all is the result of innovative applications of new technology? Or is it just another example of using new technologies to make public services more efficient and user oriented, where the changes in government organisations have been planned and controlled? Our study aims at analysing the developments steps and to identify what type of changes that have taken place and what have been the consequences of these changes, both in the central government, for the individual institutions involved and for the students.

This paper is structures as follows. In the next section we present our theoretical framework, followed by an analysis of the different phases in NUCAS

1 In Norwegian the name is Samordna Opptak (SO), see http://info.samordnaopptak.no/.
2 NUCAS has been awarded several prices, e.g. eNorge-award in 2004.

development processes. In the last section we discuss our findings compared with previous research in the field.

Theoretical perspectives

Even if computers have been used in public administration for several decades, the term electronic government (e-government) came into use rather recently. To day, government at all levels across the globe have adopted e-government systems in ways that apparently have changed their internal organisation as well as their interaction with their environment. It seems furthermore to have become commonly accepted to see e-government as a way to reform public administration, not least from a political point of view (se e.g. Fountain 2001, Grønlund 2003, Coleman 2008, Davis 2008).

By *administrative reform* we understand it «as an effort to bring about dramatic change or transformation in government, such as a more responsive administrative structure, greater rationality and efficiency or better service delivery to citizens» (King and Kramer (2008, p 2). Even though this definition does not include the use of new technology, we will to day hardly think of reforming public (or private) institutions without the extensive use of ICT.

E-Government research is not yet a research domain on own. It is also being questioned whether it should be. Scholl (2008) claims that e-Government research at best is multidisciplinary, in that it involves multiple disciplinary communities, and attempts to approach the phenomenon from the perspectives of different disciplines. E-government has traditionally been seen to include computer and information system research along with public administration and political science. However, as the structure and functioning of the public sector are to a large extent regulated by laws and regulations, reforms will most likely involve (or even depart from) changes in legal arrangements. We see that such reforms will include both technical developments along with changes in organisational structures and not least legislative reforms, see e.g. Fountain (2001), Grønlund (2003). This is illustrated in figure 1 below, where we emphasize the close interrelationship between these three elements; new technical solutions requires changes in legislation as well as the need for new organisational pattern, or the other way around (see e.g. Jansen and Schartum 2007). The direction of impact is however not unambiguous; new legislation may lead to organisational changes that are supported by new ICT systems (Sjøberg 2006), or the other way around (Johnssen 2006). We have thus to identify the different patterns.

Hovy (2008) claims that since eGovernment research is interdisciplinary, it should include both normative perspectives (as analysis of political goals and

values, legislation etc.), *technological* elements (as discussions about construction and implementation issues etc.) and *evaluative* elements (as e.g. studying the effects of introducing new technical solutions and organisational patterns). This paper aims at including all three elements, though to a limited extent. We will investigate whether changes in educational policies and legislation, initiated by politicians have caused the development of new technical solutions and organisational changes. At the same time, we want to see to what extent the drive towards using modern technology actually has been a catalyst or motivator for these changes.

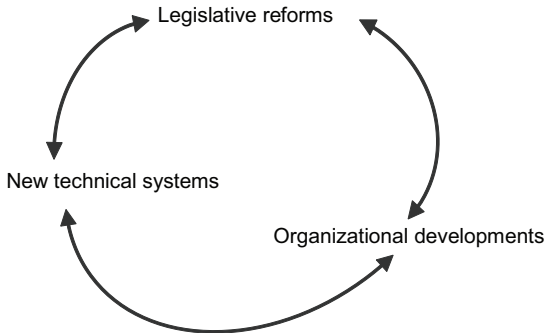


Figure 1: Elements in an administrative reform process

How does technology matter?

Through an extensive review literature on ICT and government, Kraemer and King (2008) have examined whether ICT has been an instrument of administrative reform in the U.S. They conclude that this has not been the case in the history of ICT and government in the US. Instead of being an instrument of reform, they claim «that ICT has served the interest of those in power and has supported existing administrative and political structures». In their analysis, they have listed four propositions as key component of their reform hypothesis, which we believe may be fruitful to test. Their propositions are[3]:

3 In the present version of the paper, we will discuss the three first propositions.

Reform Prop.1: Computers have the potential to reform public administration and their relations to their environments

Kraemer and Kings findings were: «*Experience with information technology and administrative reform has shown technology to be useful in some cases of administrative reform, but only in cases where expectations for reform are already well established. ICT applications do not cause reform and cannot encourage it where the political will to pursue the reform does not exist* (op cit. page 6).

In order to test this proposition, we have to identify whether reforms have takes place, and if so, how and why they have been implemented.

Reform Prop. 2: Information technologies can change organisational structures and, thus, is a powerful tool for reform

The question is whether new IT solutions have contributed to reforms other than those planned, e.g. if there have been «bottom-up» forces that influenced organisational structure and division of labour. Kraemer and King claim that, based on vast empirical evidence that that the main impact of IT applications has been to reinforce existing structures of communication, authority and power in organisations, whether centralised or decentralised. Their findings are: *IT applications have brought relatively little change to organisational structures and seem to reinforce existing structures* (op. cit. p 8).

Reform Prop. 3: Properly used, IT will be beneficial for administrators, staff, citizens and public administration as a whole

Kraemer and King claim that empirical evidence suggests that those who control IT deployment and applications determine whose interests are served by the technology. Their findings are: *the benefits of IT have not been distributed evenly within the government organizational functions. The primary beneficiaries have been functions favoured by the dominant political-administrative coalitions in public administrations and not of those of technical elites, middle managers, clerical staff and ordinary citizens.*

This implies that we must analyse for what and how the technical solution have been developed, and who they might serve.

Research model and methods

This research is based on an *interpretative* case study, in that we have based our data on an investigation of the development in one single organisation.

Departing from the hypothesis stated above, the units of analysis are technical achievements as new solutions, the bureaucratic reform processes and the corresponding changes in legislation. The empirical data in this study are collected from various documents describing the project development phases along with government reports. However, the most important sources are stories told by actors that have been closely involved in this development process. The strength is the proximity to the actual case.

This data collection method has challenges related to reliability. One problem is thus that the main informant[4] has been close related to the project, which implies uncertainty related to the bias and accuracy of the data. The data are also collected long time after the project was ended. Important facts or viewpoints may be forgotten, or the significance of conflicts may be under- or overestimated. We do, however believe that the available data provide us with substantial insight into this project.

NUCAS and the Norwegian educational system

To day, NUCAS coordinates the admission to regular undergraduate studies in Norway. However, this has not always been the case. The present organisation and administrative routines are the result of more that 40 years of development, even if the last 16–17 years have been the most important in the context of our analysis.

It is thus important to see the NUCAS process is the continuation of a long range of reforms that started in the 1960'ies with the growth of the regional university and state colleges in Norway[5]. The result of this process was that more than 100 educational institutions were distributed all over Norway. The implication was a mass education revolution in Norway, resulting in an increase from about 10 00 students in 1960 to 41 000 student that were enrolled in 1988. However, the application and admission routines were at that time fully decentralised. Each student had to submit his/her application to each individual institution, and there was no central registration system that could provide the central authorities with necessary information in order to survey and control application and admission systems.

4 One of the authors (Einar Løvdal) has been head of development project from 1991 to present, while the other author may have interpreted these reform processes in the context of his own experiences from being a civil servant working with IT policy in the government.

5 The Ottosen-committee presented 5 reports in the period 1966–70, which became a basis for the development of higher education that started its expansion in 1970 with developing the regional higher colleges.

A perceived crisis in our higher education led to the appointment of the Hernes committee. Their report[6] proposed a rather dramatic reorganising of higher education in Norway. One element in their proposals was to reduce the number of colleges and to build a Norwegian Educational network («Norgesnettet») between the universities, university colleges and regional college centres. This idea was, with some modifications, implemented in the period 1993–1994.[7] Another very important element was the harmonising of regulations for universities and regional colleges, resulting in one unified law for the whole sector. This law became essential for the development of the admission handling system.

New reforms were following. In the context of this paper, the «Quality reform» [8] from 2003 is essential, as it defined a completely harmonised framework for the whole sector, based on 3-years bachelor and 2-years master programs[9]. Various administrative systems have been developed to support the implementation of this reform, which also have implied the formalisation and bureaucratization of routines and functions in the administration of the students at the individual institutions. These have, however, been one of the objectives of this reform; on the one hand to make visible the rights of the students and at the same time carry out much rigorous control of their progress. These reforms have, as we will see, had decisive influences on the application handling and admission system, both on the entrance requirements, on the structure of the different educational programs and how the different institutions became more professional in their administrative work.

The NUCAS development process

The revolution (or may be it became an evolution) of the admission system thus originated from a rather chaotic situation in about 1990, where all case handling were fully decentralised and no one did know the number of real applicants each year. A committee[10] was appointed, which handed over its report in December 1990. The result was that the SO-project was established. The goal of SO-project was to develop a complete new administrative system that could

6 The Hernes report NoU 1988: 28 «Med Viten og Vilje».
7 See St. mld 40 (1990–91) Om høyere utdanning.
8 St.meld. nr. 27 (2000–2001) Gjør din plikt – Krev din rett Kvalitetsreform av høyere utdanning.
9 Se http://www.regjeringen.no/pages/2033172/PDFS/STM200720080007000DDDPDFS.pdf
10 This committee was appointed by the ministry and headed by Professor Bjørn Pedersen, UiO

- Provide a national information system including statistics for analyzing the demands for higher education.
- To establish a national wide computer network (UNINETT) to connect the all institutions.
- Start developing pilots for ICT-based admission system that could help the weaknesses and inefficiency of the existing decentralized and uncoordinated routines for handling of applications.

A short overview of the different phases in the development process in given in figure 1 below:

1991	The SO-project established, based on the Pedersen-report
•	The development of a information system for centrally registration of all applicants to higher education in Norway
1992 -94	Pilot projects based on a new coordinated, distributed model for admission handling
•	Selected case handling, SO-project responsible for the coordination og central services
•	A new, co-ordinated regulations of rankings for colleges, replacing 17 old ones
1995	A common law for universities and university colleges
•	Generel competence requirements as basis for admission to higher education
1996-97	Implementation of the National coordinated Admission Model (NOM)
•	National available electronic application handling and admission services available for all
2000	Implementation of automatic case handling based on electronic diplomas
•	Full case handling across Universities and colleges from 2000
2000	First year with of submission of application etc. via Internet (”søkerveven”)
2001	The *Competence* reform is implemented
2002	The SO organisation takes over operations and maintenance of the National Diploma database

Figure 1 The Milestones in the NUCAS development project

A crucial step of this development process was the design of the NOM[11] model, which is a combination of central coordination and service provision along with local responsibilities at each individual institution. This model, which allows for that the individual local institution may handle application to other institutions, requires standardised admission rules and close co-operation between them.

11 NOM is the abbreviation in Norwegian of a National admission Model (Norsk Opptak Modell)

On should not underestimate the importance of the development of an ICT-based infrastructure for communication and exchange of data between the co-operating institutions., The UNINETT was build as an advanced computer network which provided important services as electronic mail and file transfer, which could replace the physical transport of floppy diskette.

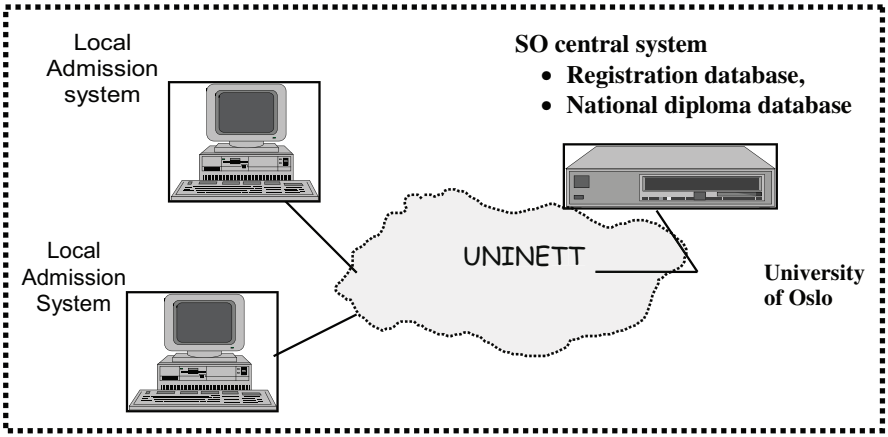


Figure 2 The National Admission Model

The later stages in the development was

- To eliminate paper communication and the need to send paper documentation for the great majority of applicants, this was made possible by the introduction of electronic diplomas.
- Fully automated case handling for the great majority of applicants – no manual case handling.
- Immediate admission offer or admission guaranty for those fulfilling admission criteria.
- Requires a simplification and revision of admission regulation – planned by 2009.

Thus, there is (was) an urgent need for a standardised public available electronic signature that can secure electronic authentication and signature.

The structure of the NUCAS electronic system

This information system, the NUCAS «admission machine», may be illustrated in this way:

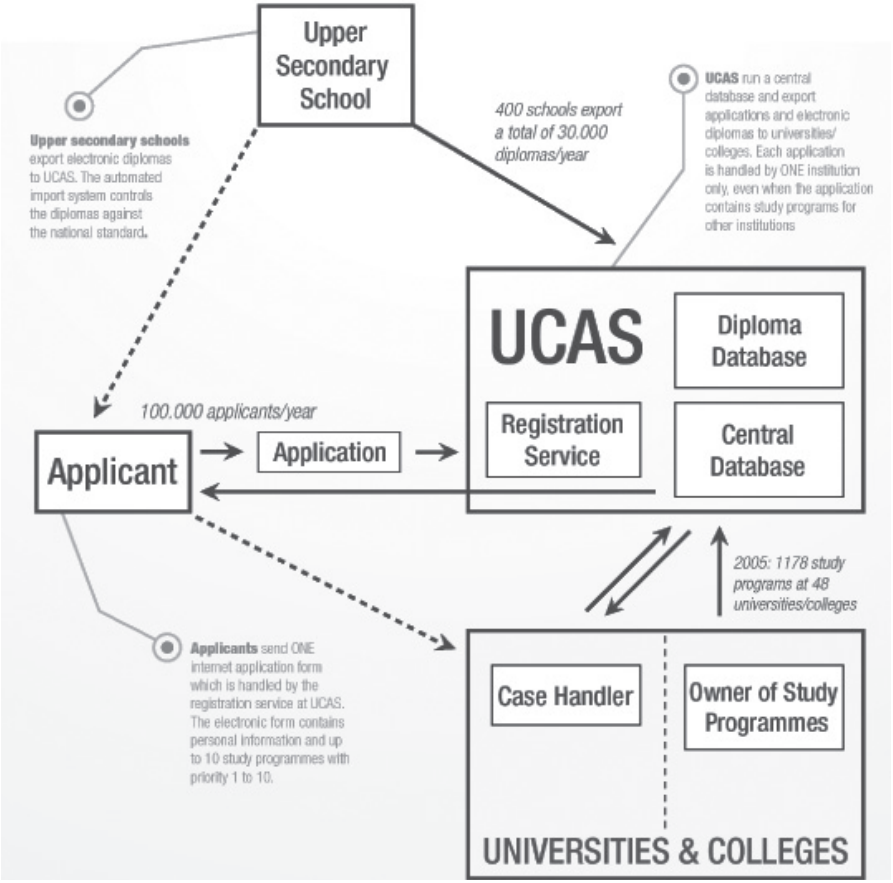


Figure 3: The NUCAS admission machine

Figure 3 illustrates that data on the applicants are collected from various databases, among them a register containing electronic diplomas from secondary schools. These data are exported to the local administrative systems at the individual universities and colleges, and furthermore used by e.g. the Norwegian State Educational Loan Fund when handling application for financial support.

In this respect, the NUCAS admission machine can be seen as a *hub* for many other administrative systems in the educational sector.

Technical challenges

A basic «brick stone» for this system was the development of a new *data model*, containing a formalised and codified representation of all existing rules and regulations related to the admission procedures, including competence and ranking data bases (with formalised representation of all competences related to admission and the algorithms for ranking the applicants at the individual institutions[12] for all types of educational programs). This data model has been instrumental for supporting the local application and admission handling systems. Another challenge was clearly the development of *electronic diplomas*, which implied the formalisation of a very complex set of rules along with a large number of programs in secondary schools.[13]

Close co-operation between main actors

Seen from the viewpoint of the SO-project, it has been a well-defined division of work and responsibilities between the Ministry of Education and Research, the NUCAS central service and the institutions of higher education. An important feature of NUCAS system is the strong coordination of all phases of the admission process:

- *One application form* per applicant only, even when applying for admission to study programs at different universities and colleges.
- *One case handling institution* per applicant only, thereby eliminating duplicate work even when the application contains study programmes at several institutions.
- *One final admission offer* per applicant, to the highest prioritized study programme where he/she meets admission criteria.
- Coordinated *centralized registration* of application in combination with *decentralized case handling* and final *centralized selection procedures* (the NOM model).

12 The robustness of this database was illustrated when the Parliament (Stortinget) in the late spring 1999 revised the admission rules to include credits for having completed military service. This change was easily implemented in the admission «machine» early in July same year, thus into effect almost immediately.

13 The reform 94 included more than 200 different «programs», that is legal combinations of courses at secondary schools.

While the 3 first features were included in the original Pedersen report from 1991, the last feature, the realisation of the NOM model, has only been possible through the design and implementation of the rather sophisticated technical solution that grew out of the pilot projects from 1993–1996.

The role of the central authorities

The SO-project has been a cooperative effort, where the Ministry of Education and Research have played an instrumental role in funding the NUCAS central service, and in implementing the necessary revisions in legislation and other regulations covering application procedure and admission criteria. In this way, we may say that the SO-project has been mandated and controlled by the central authorities, following political decisions made by the parliament. However, there has been a fruitful co-operation between the various actors in this project. These are the achievements;

- No duplicate evaluation work – as average number of institutions involved in admission work per applicant drops from 3.5 before 1995 to currently less than 1.1.
- 84% of students entering higher education receive their admission offer in the first round of the national selection, while 97% receive it before middle of August.
- Case handling is semi-automatic by means of electronic diplomas, covering 66% of qualified applicants
- The collection system for electronic diplomas now annually covers 97% of pupils finishing secondary school.
- Improved service levels and quality both for the applicants, for the universities and colleges, and for the public authorities.
- Even lowering the costs spent on admission work at all levels.
- Efficiency is achieved by use of Internet services and semi-automated case handling

For *central management,* the system implies that they will have updated statistics on the number of applicants and admission each program. It is even possible to analyse the effects of specific regulation measures, and therefore aim to tune the admission criteria in various ways.

For the *local institutions* the new system has reduced and simplified the admission process. It is also important that short time after the application deadline they will know how many students that have applied for admission to each program. Thus, they may initiate additional recruitment actions. They have also the opportunity to marketing their specific programs to targeted

student groups. Schools with specific admission requirements are allowed to manage these themselves.

For *the student* the system offers a much simpler and quicker admission process. They can retrieve updated information on all programs when they need it, they will have access to all admissions rules and procedures, and they may check the probability for being admitted to the selected program, based on statistics from previous years. The admission procedure is fairer, as the bested ranked students cannot book more programs, as they have to choose one single first priority.

The combination of centralised and decentralized case handling offers opportunities for better quality control of data. It is also much more difficult to cheat the system, as electronic diplomas are collected automatically from the high schools, and sent to the local institutions. Both for the ministry/directorate and the institutions, this has contributed to greater efficiency and less errors.

Analysis and discussions

What are the main elements of this reform process? One way of illustrating this may be:

Time period	Situation in the educational sector	Political changes in regulations	Administrative – organisational actions	Milestones in technical developments
1970–90	Increasing growth and complexity	End of college expansion The Hernes committee was appointed in 1988	No specific action due to lack of effective means for regulation and control	Development of local administrative systems – no interaction between these system
1990–94	Implementation of the Hernes proposals	Pedersen report proposed the development of a MIS for control Harmonisation of admission& ranking procedures	Establishment of SO-project. Development of the NOM-model as basis for the reform work.	UNINETT in operation Development of MIS Pilot projects are carried out.
1995–99	Norgesnettet Reform 94	A unified law for the whole higher education sector	Consolidating SO-project and local admission offices	Implementation of new data model and admission machine. Pilot version of web-based information system
2000–02	Competence [1] reform	Implementation of new rules for admission etc.	Full electronic coordination of admission handling	Web-based application system National diploma data base

2003-	Quality reform	Harmonisation of higher education into bachelor and master program	SO becomes an permanent organization	Application and admission handling is 90% automated

Table I: Development of NUCAS – political, organisational and technical actions

This table may indicate that the organisational and administrative changes, supported by adequate technical solutions, have been the result of overall planned actions. However, when looking closer into this development history, it seems evident that technical achievements along with local initiatives have been influential in the design and implementation of the reform process, and that the results are different from what was originally planned.

It is important to understand how all three parties have influenced the development and reform processes in various ways. Even though the ministry and the political system had an overall control, the technical oriented initiatives as well as the local institutions, including the administrative staff have been instrumental. While the central authorities mandated the Pedersen report and defined the general setting for the development work and implemented the necessary changes in laws and regulations, it is likely that the technical project along with the institutions have influenced both the revisions in regulations (through the work with the new data model) as well as the establishment of SO as a government agency.[14] In particular have the design and development of the admission machine and web-based application case handler been important in the implementation of the overall solution. Without a successful technical and organisational solution, it is not likely that the SO-project had become a permanent organization

Result and effects of the work

We have stated that the goals that were defined for the project have been fulfilled. But who have actually benefited from this reform; the ministry, the institutions, the students or the society at large? As we have seen, the SO-project, which was initiated with aiming at providing a management for the central authorities, turned out to be an automated, partly distributed decision system. This process has been supported by the necessary changes in legislation, and by the establishment of the SO as a central agency. However, this had not been possible without the success of the technical development and implementation

14 Oral report from meeting between the SO-project and the Ministry of Education, has to be verified.

work, which also have had support from the local admission offices. The introduction of the Competence reform as well as the Quality reform has also implied new requirements to the SO. On the other hand, the robustness and flexibility of the SO system, in that it has been able to implement these reforms in an effective way has consolidated SO as organisation. It has also supported the techno-bureaucratic management and control of the students.

Our findings are summarized in the table below.

Actor groups Goals and effects	Central government	Local institutions	Students /others
Management tool	The MIS provided a adequate tool for management	The MIS turned out to be useful at a local level It supports local case handling based on standard criteria	The Web-based information system is useful in the planning of applications
Regulation and control	Admission machine supports the implementation of changes in ranking and priorities	The data from NUCAS is being used in administering and controlling the students	Both positive and negative The students can easily get all information they need. Their flexibility are reduced
Efficiency and effectiveness	Administrative work is become less demanding	Less resources used for application handling admission management	Yes, the application and admission process is much simpler and demands less efforts
Other benefits	The use of advanced technology is viewed as goal on its own	This system is also useful in attracting new students and local marketing	It also supports the rights of the students

Table 2: Goal, benefits and effects of the NUCAS system for different actor groups

Concluding discussion

Do our findings conform to the propositions that were formulated by Kraemer and King?

Prop.1. Computers have the potential to reform public administration and their relations to their environments

Our analysis has show that the reform process was initiated and actively supported by the ministry, based on political decisions. The results of this reform are to a large extent what were planned. The NUCAS system, along with other systems has strengthened the ministry and central management's capabilities for control and regulation. However, there are clearly results that go beyond the primary goals, which can be contributed to the application of new

technology. We cannot, however claim the new technologies have driven this reform on its own. We conclude that the proposition is partly supported, and that our findings are not in accordance with Kramer and King's findings.

Prop. 2. Information technologies can change organisational structures and, thus, is a powerful tool for reform

Our analysis has shown that some organisational changes have been planned by the ministry. On the other hand, the NOM model and even the SO organisation seem to be the result of successful ICT-based innovation supported by local interests, and would not have been feasible without these technical solutions. The proposition seems to be supported, which implies that we disagree with Kramer and King findings.

Prop. 3 Properly used, IT will be beneficial for administrators, staff, citizens and public administration as a whole

Our findings as summarized in table II show that NUCAS has been beneficial for both the central management, for the staff at the local institutions, for the students, and even for the society at large. Even though the system allows for efficient ruling and control, it does also serve other interests. Proposition 3 is supported, while we disagree with Kramer and King

Our main conclusions are that there is no clear rejection for any of the propositions, rather the opposite; they are at least partly support. We do, however, not claim that these hypotheses can fully explain the reform processes in the NUCAS developments. On the one hand, there is no doubt that political and central management priorities have been decisive in this reform. At the same time, we have to acknowledge the power inherent in the visions that technological developments creates. Such visions, combined with enthusiastic development team and supportive managers in the various local institutions seem to have created an environment for innovative technical and administrative solutions.

To what extent may these finding be generalized? Our case is particular in the sense that it is about the development of a new, specific system. It has been selected for this study because it succeeded in fulfilling political goal, even goals that were not defined at the outset. One may say that it has been a complete match between technical achievements, organisational developments and political ambitions. The creation of a new organisation may be an «easier» administrative reform process (even though it also implied substantial changes in existing rules and procedures), than to implement radical changes

in existing one. We believe that another, very important factor has been that the government agencies involved in this reform process are subordinate to the same minister. This implies that it has been an inter-organisational reform, but not cross-sectorial, which is much harder to accomplish.

However, the are most likely a number of lessons to be learned about how to carry out this type of technical development work and administrative reform process in general that we believe are useful to others.

References

Coleman, Stephan (2008) Foundations of Digital Government. In *Digital Government. E-government research, case studies and Implementations Springer*, New York

Davis, Sharon (2008) Introduction to digital government research in Public policy and management, In *Digital Government. E-government research, case studies and Implementations* Springer , New York

Flak, Dertz and Jansen (2008) *Teknologi som drivkraft for utvikling av norske kommuner* In Jansen og Schartum (ed) *Elektronisk forvaltning på Norsk*. Fagbokforlaget

Fountain, Jane (2001) *Building the Virtual State Information Technology and Institutional Change*. Washington, D.C. Brookings Institutions Press

Fountain, Jane (2002) *Information, Institution and Governance* Cambridge. Harward University

George, J.F. and King, J.L (1991) *Examining the computing and centralization debate* Communication of the ACM 34(7)63–72

Hovy, Eduard (2008) An outline for the Foundation of Digital Government Research. In *Digital Government. E-government research, case studies and Implementations* Springer, New York

Johnssen, Gustav (2006) E-forvaltning och lagstiftning i Sverige 2000–2006. In Schartum (red.) *Elektronisk forvaltning I Norden* . Fagbokforlaget, 2006

King, J. L. and K. L. Kraemer (1985) *The dynamics of computing* New York. Columbia University Press

Kraemer, Kenneth and John L. King (1986) Computing and public organizations *Public Administration Review* 46(6) 488–496

Kraemer, Kenneth and John. L. King (2008) Information Technology and Administrative reform. Will Government be Different? In Norris (ed) *E-Government Research . Policy and Management* IGI Publishing , Hershey, New York

Laudon, K. (1974) *Computers and bureaucratic reforms*. New York, John Wiley & Sons

Løvdal, E. (2008) Samordna opptak Norge samlet til ett utdanningsrike. I Arild Jansen og Dag Wiese Schartum (red.) (2008) *Elektronisk forvaltning på Norsk*. Fagbokforlaget, Bergen. ISBN 978–82–450–0554–7.

Marche, S., & McNiven, J.D. (2003) E-government and e-governance. The future isn't what it used to be. *Canadian Journal of Administrative Science,* 20(1), 74–86

Stensaker, Bjørn (2006): *Institusjonelle kvalitetssystemer i høyere utdanning – vil de bidra til bedre kvalitet?*Evaluering av kvalitetsreformen: Delrapp.2, NIFU Oslo

Scholl, Hans J. (2008) Discipline or Interdisciplinary Study Domain= Challenges and Promises in Electronic Government research . *Digital Government. E-government research, case studies and Implementations Springer* , New York

Sjøberg, Cecilia Magnusson (2006) Rätt rättsinformasjon i e-forvaltningen. In Schartum (red.) *Elektronisk forvaltning I Norden* . Fagbokforlaget, 2006

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

SYSTEMUTVIKLING I RETTSLIG PERSPEKTIV*

Dag Wiese Schartum

1 Beslutningssystemer, beslutningsstøttesystemer og saksbehandlersystemer

I innledningskapittelet ble det understreket at utvikling av elektronisk forvaltning ikke kan begrenses til teknologiutvikling, men at også utvikling av organisasjon og regelverk er viktige elementer. For mange er det selvsagt at teknologiske og organisatoriske spørsmål er nært knyttet til hverandre, og at organiseringen ofte må endres dersom det skal være mulig å gjøre hensiktsmessig bruk av IKT. Det er nok ikke like innlysende for alle at regelutvikling må stilles opp som et likeverdig utviklingselement. Riktignok fremstår regelverk ofte som et hinder for teknologisk og organisatorisk endring, og slik sett er jus anerkjent som generelt relevant i eForvaltningsprosjekter. I dette kapittelet er perspektivet imidlertid langt bredere. For det første vil jus både bli diskutert ut i fra perspektivet «hinder» og «muliggjører». For det andre er et helt sentralt poeng at forvaltningens oppgaver i meget stor grad er rettslig styrt, noe som innebærer at jus uansett blir viktig ved utvikling av systemer som skal brukes for å utføre rettslig styrte forvaltningsoppgaver. I dette kapittelet skal jeg gi en oversikt over rettslige spørsmål knyttet til slikt utviklingsarbeid.

I artikkelen blir hovedvekten lagt på rettslige *beslutningssystemer* og *beslutningsstøtte*systemer i forvaltningen. Som regel kan disse også betegnes fagsystemer. Betegnelsene gjelder IKT-systemer som er utviklet for å treffe vedtak i henhold til forvaltningslovgivningen. Fordi vedtakene i stor grad er lovstyrte vil de inneholde representasjoner av de rettsreglene som skal styre vedtakene. Vedtakene vil først og fremst være enkeltvedtak, dvs vedtak som er bestemmende for den enkeltes plikter og rettigheter.[1] Beslutningssystemer betegner systemer med høy grad av automatisering og kan i ytterste tilfelle tenkes å utføre enkeltsaksbehandling «uberørt av menneskehender». Beslutnings*støtte*systemer er utformet ut i fra forutsetningen om at det er et

---

* Artikkelen er tidligere trykket i Arild Jansen og Dag Wiese Schartum (red.) «Elektronisk forvaltning på norsk. Statlig og kommunal bruk av IKT.», Fagbokforlaget 2008 (417 s) – som er den nye må-ha-boken for de som interesserer seg for omstilling av offentlig sektor.

1 Jf. forvaltningsloven § 2 bokstav b.

menneske som skal treffe vedtaket og systemet skal kun ha saksforberedende funksjoner. Beslutnings(støtte)systemene er spesielt utviklet for hvert forvaltningsområde. Saksbehandlingssystemer er derimot systemer som gir *generell* støtte til saksbehandlingen vedrørende journalføring, ulike typer dokumenthåndtering, elektronisk kommunikasjon mv. Også slike systemer kan ha et rettslig innhold eller de må forholde seg til rettslige krav ellers, for eksempel slik at systemet må være i tråd med bestemmelser i arkiv- og forvaltningsloven med forskrifter. Deler av artikkelen er også relevant for saksbehandlingssystemer men disse blir ikke spesielt drøftet.

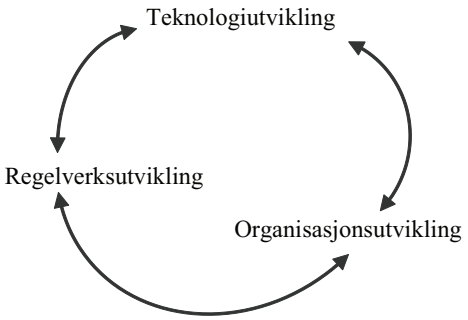
At spørsmålene er «rettslige» betyr at de må løses i henhold til krav som følger av rettssystemet, det vil for eForvaltningens vedkommende primært si forvaltningsretten. Forvaltningsretten består i stor grad av regelverk (lover, forskrifter, instrukser mv.) som fastsetter hvorledes forvaltningsorganene skal drive sin virksomhet. Når en i stor grad velger å styre forvaltningen ved hjelp av lover med tilhørende forskrifter,[2] er det delvis fordi legalitetsprinsippet og rettsstatsidealet gjør det nødvendig. Staten utøver myndighet[3] og er selv bundet av sine vedtak. Kunngjøring av vedtak og den tid det tar å gjennomføre endringer av eksisterende vedtak, bidrar til å skape forutberegnelighet og motvirker vilkårlighet. Også i andre saker enn der rettslige prinsipper gjør det påkrevet blir lovveien i praksis ofte valgt. En årsak kan være at det kan være vanskelig å ta stilling til om et vedtak kan sies å være til byrde for noen. Viktigere er imidlertid trolig at lovvedtak innebærer tydelige og grundige beskrivelser av en ønsket rettstilstand, noe som uansett kan ses som politisk fordelaktig. Jeg vil ikke her komme nærmere inn på mulige årsaker til bruk av lovgivning, men nøyer meg med å understreke at begrunnelsen kan – men ikke trenger å være – rettslig.

Vedtakelse av lover og tilhørende forskrifter utgjør en helt sentral del av den politiske styringen av forvaltningens utøvelse av myndighet, og det er slikt regelverk som vil bli viet oppmerksomhet i dette kapittelet. I tilslutning til lover og forskrifter utferdiger forvaltningen ofte instrukser om hvorledes lovene mv. skal forstås, og også slike utfyllende interne regelverk har betydning for denne fremstillingen. Også rettslige prinsipper (jf. legalitetsprinsippet, likebehandlingsprinsippet, saksutredningsprinsippet mv) spiller en vesentlig rolle fordi de kan gi bidrag til rettslige løsninger i eForvaltningen selv om det ikke foreligger konkrete lovvedtak som løser rettsspørsmålene.[4] Når jeg her

2 Gjerne gitt av Kongen eller et departement.
3 Dvs gir forbud, påbud og innskrenking av rettigheter.
4 Jeg kommer ikke spesielt inn på betydningen av rettspraksis, forvaltningspraksis og flere andre rettskilder. Lovforarbeider og -etterarbeider er imidlertid nært knyttet til slike regelverk som er sentral i kapittelet.

i stor grad setter likhetstegn mellom «rettslig» og regelverk (jf. figur 1), innebærer ikke det at andre rettskilder enn lover, forskrifter mv. ekskluderes, men at regelverk vektlegges spesielt. I motsetning til andre rettskilder inneholder lover, forskrifter og forvaltningens instrukser gjerne helhetlige beskrivelser av materielle forvaltningsordninger, samt de saksbehandlingsrutiner som skal følges når forvaltningen behandler saker. Derfor er regelverk ofte helt sentrale som «oppskrifter» på de fremgangsmåter som ellers må følges og som beskrivelser av de resultater beslutningssystemene i forvaltningen skal gi. Som jeg senere kommer tilbake til, innebærer utvikling av beslutningssystemer at det ofte er aktuelt å «oversette» eller transformere rettsreglene i lovene mv. ved hjelp av programmeringsspråk for på den måten å kunne automatisere anvendelsen av regelene, se avsnitt 4.

I figur 1 står det «regelverks*utvikling*» (kursivert her), noe som skal understreke at det ikke primært er rettstilstanden, slik den er til et gitt tidspunkt som er hovedtema i dette kapittelet, men hvorledes regelverket *endrer seg* i forhold til forandringer i teknologi og organisering. En viktig kritikk mot lovgivning er at den er tidkrevende å endre. I et eForvaltningsperspektiv er det imidlertid like viktig at lov- og forskriftsendringer kan forekomme relativt hyppig og derfor er en viktig del av utfordringen å vedlikeholde og videreutvikle systemløsningene. Selv om en kan være irritert over den tid det tar å endre loven, vil forvaltningen i tillegg trenge tid til å implementere lovendringene i egne systemer mv., for eksempel ved at nye regler transformeres til programkode i forvaltningsorganets beslutningssystem. I den elektroniske forvaltningen er det derfor viktig å erkjenne at en er under politisk styring, og at denne styringen i stor grad skjer gjennom lovgivning som er bindende for forvaltningen selv, og som derfor må implementeres i forvaltningsorganenes systemløsninger innen fastsatt tid for ikrafttredelse.



I det følgende vil jeg først drøfte hvorledes regelverksutviklingen kan sies å påvirke systemutvikling, dvs. av hvilke systemer som blir utviklet, med hvilket innhold, på hvilke måte mv. Temaet gjelder med andre ord rettslig styring av IKT i offentlig forvaltning, se avsnittene 2 og 3. I avsnitt 4 redegjør jeg for hovedpunkter i prosessen å transformere lovtekster mv. til programkode. I avsnitt 5 er temaet mulig påvirkning av teknologien på lovgivning (jf. «automatiseringsvennlig lovgivning»), mens jeg i avsnitt 6 gjennomgår hvorledes analyser fra systemutviklingsarbeider kan gjøre det mulig å skrive bedre lovtekster. Forholdet mellom regelutvikling og organisasjonsutvikling (og viseversa) blir kort behandlet samlet i avsnitt 7 og har teknologiutvikling som bakgrunn og ramme. Det avsluttende avsnitt 8 gjelder mer generelt juristers rolle ved utvikling av rettslige beslutningssystemer i forvaltningen.

2 Virkninger av regelverksutvikling på systemutvikling

2.1 Innledning

Målet her å gi et innblikk i noen hovedaspekter knyttet til den rettslige – direkte eller indirekte – styringen av systemutvikling i elektronisk forvaltning. Temaet er med andre ord bruk av lover og forskrifter for å styre utvikling av IKT-systemer i forvaltningen. Ved behandlingen av forholdet mellom jus og systemutvikling har jeg valgt å ta utgangspunkt i forestillingen av lovregler som hindring for teknologisk utvikling. Dette er en vanlig innfallsvinkel til forholdet mellom jus og IKT – ikke minst innen offentlig forvaltning, se avsnitt 2.2. Valget av utgangspunkt gjør det nødvendig å balansere bildet ved å ta opp spørsmål om bruk av regelverk for å *legge til rette* for (muliggjøre) utvikling av hensiktsmessige og ønskede systemløsninger (avsnitt 2.3).

Et slikt skille mellom regelverk som hinder og muliggjører er ikke alltid enkelt å håndtere blant annet fordi det som fremstår som hindring i et perspektiv kan være muliggjørende i et annet perspektiv – og omvendt. Krav i lovverket om samtykke fra enkeltpersoner er for eksempel et hinder for forvaltningsorganer som ønsker å utvikle systemløsninger der den enkelte part ikke er tiltenkt noen aktiv rolle i saksbehandlingen. Ønsker forvaltningsorganet i stedet å utvikle løsninger som i størst mulig grad er basert på *selvbetjenings*prinsippet, kunne den samme rettslige reguleringen imidlertid fremstått som noe positivt. Omvendt kan krav til sikring av elektronisk kommunikasjon i utgangspunktet ses på som noe som legger til rette for slik informasjonsutveksling, dvs. noe positivt. Blir kravene uforholdsmessig dyre/tungvinte kan de imidlertid i stedet oppleves som hindring.

2.2 Regelverk som hindring i systemutviklingsarbeid

Det går et viktig skille mellom regelverk som er vedtatt med tanke på den aktuelle type systemløsning eller bruk av teknologi, og regelverk som er gammelt og eksisterer uten at det er gjort noen slike vurderinger. I først nevnte tilfelle er det tale om en direkte og konkret styring av teknologi – mislykket eller vellykket. For eksempel ble det innført forbud mot direkte markedsføring ved hjelp av telekommunikasjon mv. i personopplysningsloven og markedføringsloven som respons på at det var utviklet en praksis som ble ansett som uakseptabel.[5] I sist nevnte tilfelle er det tale om lovgivning som er gitt uten tanke på situasjoner vedrørende elektronisk forvaltning. Inntil revisjonen i 2002[6] var for eksempel bestemmelsene i forvaltningsloven ikke vurdert eller utformet med tanke på elektronisk kommunikasjon, noe som skapte problemer fordi flere bestemmelser forutsatte tradisjonell skriftlighet og/eller underskrift.[7]

Det generelle poenget er at systemutvikling, gjerne i samband med organisasjonsutvikling, ofte vil innebære forslag til nye arbeids-/fremgangsmåter. Slike forslag til løsninger vil derfor kunne aktualisere rettsspørsmål som ikke har vært vurdert da loven ble gitt. Fordi situasjonen er ny, kan det også være vanskelig å ha klare holdepunkter for hva lovgiver ville ha ment om spørsmålet. Et rettsspørsmål kan med andre ord formelt og teknisk sett være regulert, men på en måte som ikke tydelig hviler på en aktuell politisk/faglig vurdering. Taushetspliktbestemmelser kan for eksempel fremstå som foreldede fordi de var vedtatt i en tid da organisering, arbeidsdeling og muligheten for å kontrollere personers tilgang til opplysningene var en helt annen enn i den aktuelle situasjonen.

Samtidig som systemutvikling kan begrunne fornyet vurdering av lovgivningen, kan terskelen for igangsetting av lovarbeider være høy og dessuten kreve langt mer tid enn det som lett lar seg passe inn i et igangværende systemutviklingsarbeid. En mulig «løsning» på en slik konflikt er at forvaltningen unngår å fremme forslag om systemløsninger som kan være i strid med gjeldende lovgivning. En annen mulighet er at en går langt i å fortolke eksisterende bestemmelser analogisk eller innskrenkende og derved legger lovforståelsen «på strekk», noe som kan gi løsninger som i verste fall kan vise seg å være ulovlige.

---

5 Se henholdsvis personopplysningsloven § 26 og markedsføringsloven § 2b.

6 Se Ot.prp. nr 108 (2000 – 2001) om lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon.

7 Fortsatt er ikke forvaltningsloven vurdert og utformet med tanke på elektronisk saksbehandling for øvrig, se for eksempel Dag Wiese Schartum: Møte mellom forvaltningsretten og personopplysningsretten, I: Schartum (red.) «Elektronisk forvaltning i Norden», Fagbokforlaget 2007.

En tredje angrepsvinkel er å gå veien om lovgivnings- og/eller forskriftsendring, dvs slik at spørsmål om endring av lov og/eller forskrift reises og gjennomføres i sammenheng med systemutviklingsarbeidet. Ofte vil det imidlertid være ønskelig å gjennomføre utviklingsarbeidet (langt) raskere enn det endringer av lov og forskrift normalt krever. I dag er det ikke gitt noen særlig instruks eller retningslinjer vedrørende lov- og forskriftsendringer som direkte er foranlediget av at forvaltningen utvikler informasjonssystemer. Etter min mening er det et poeng å undersøke om det kan være akseptabelt med mindre tidkrevende fremgangsmåter i tilfelle av små endring av lov og forskrift når bakgrunnen er utvikling av eForvaltningsløsninger. Dermed kan faren reduseres for at forvaltningen legger tvilsomme rettsoppfatninger til grunn for systemløsningene. En annen mulighet er å starte analyser av behovet for regelendring så tidlig som mulig, gjerne som del av arbeidet med å utforme mandat for den prosjektgruppen som skal utvikle systemet. På den måten kan en i alle fall redusere risikoen for forsinkelser.

Når det har skjedd en rettslig regulering med tanke på en bestemt teknologi eller bruk av teknologi, er situasjonen i utgangspunktet en helt annen enn tilfelle der gammel lovgivning får effekt på forslag om nye systemløsninger. I først nevnte tilfelle kan man hevde at hindringen ikke er annet enn resultatet av lovlige, demokratiske politiske beslutninger som derfor i utgangspunktet må respekteres. Jo mer konkret og spesifikk reguleringen er, desto sterkere kan dette argumentet anses å være.

2.3 Regelverk som muliggjører for systemutvikling

Lover og forskrifter er blant de viktigste virkemidlene staten rår over. De kan håndheves ved hjelp av rettssystemet og i siste instans kan det settes makt bak kravet om gjennomføring (bøter, fengsel, erstatning mv.).[8] Derfor er det ikke overraskende at slike regler ikke bare er aktuelle som «hindre» men også kan brukes som en støtte og forutsetning for utvikling av elektronisk forvaltning. Her vil jeg trekke frem fem typer muliggjørende bruk av regelverk. Det er ikke uten videre alltid lett å stille opp klare skiller mellom de kategoriene jeg introduserer, og ett og samme regelverk kan fylle mer enn én funksjon, noe bl.a. eForvaltningsforskriften[9] er eksempel på.

Regelverk kan for det første slå fast at det er lovlig å anvende elektroniske hjelpemidler i offentlig forvaltning. At noe fastsettes som lovlig innebærer

8 Dette forutsetter riktignok at rettsregelen faktisk håndheves, men forutsetningene for håndhevelse kommer jeg ikke nærmere inn på her.

9 Forskrift av 25. juni 2004 nr. 988.

også en klart signal om at det er aktuelt og kanskje også forventet å anvende IKT på disse måtene. Endringer i forvaltningsloven i 2002 klargjorde for eksempel at elektroniske signaturer kunne erstatte underskrift og at krav til skriftlighet kunne være tilfredsstilt ved bruk av elektroniske dokumenter.[10] Forvaltningsloven og eForvaltningsforskriften inneholder flere bestemmelser som klargjør at elektronisk kommunikasjon er lovlig i flere sentrale situasjoner.[11] Det kunne kanskje vært mulig å komme frem til samme resultat ved hjelp av en fortolkning av forvaltningslovens bestemmelser, rettspraksis, forvaltningsrettslige prinsipper mv. I så fall ville det imidlertid lett være knyttet tvil til resultatet, og dermed usikkerhet som kunne hemmet utvikling av elektroniske kommunikasjonsløsninger.

For det andre kan det tilrettelegges for bruk av elektroniske løsninger ved at forvaltningsorganer gis kompetanse til å stille formkrav og krav til fremgangsmåter mv. som innebærer bruk av IKT.[12] Tollforskriften gir for eksempel anledning for spedisjonsfirmaer mv. til å søke om å kunne foreta elektronisk overføring av tolldeklarasjon til tollvesenets ekspedisjonssystem. Dersom tillatelse gis etableres det samtidig en plikt til å benytte slike fremgangsmåter.[13] På lignende vis[14] åpner forskrift til ligningsloven for prøvedrift med elektronisk oppgaveinnlevering for næringsdrivende.[15] I andre tilfelle er departementet eller annen myndighet gitt kompetanse til å fastsette hvorledes skjemaer mv. skal se ut og at skjemaer skal innleveres i maskinlesbar form. Finansdepartementet har således hjemmel til ved forskrift å fastsette krav til maskinlesbare skjemaer etter ligningsloven § 6–16.[16]

For det tredje kan bestemmelser bidra til å redusere risiko ved å bruke IKT. Lov om elektronisk signatur[17] har for eksempel som formål å legge til rette for sikker bruk av elektroniske signaturer ved å fastsette krav til kvalifiserte elektroniske signaturer og generelt avklare rettsvirkningene av elektroniske

10 Se fvl § 2 første ledd bokstavene g og h.

11 Se særlig §§ 5, 7, 8, 9, 10 og 11.

12 I ett tilfelle har en norsk regjering til og med ved kongelig resolusjon pålagt bruk av en bestemt teknisk standard. Dette skjedde i 1991 ved kgl. res. av 6.12.1991 da Arbeids- og administrasjonsdepartementet fikk kompetanse til å kunne pålegge statsforvaltningen å bruke standardprodukter i løsninger for datautveksling mellom sine edb-systemer. I dag er IP/TCP med mer (InternetProtocol) som fundament for NOSIP.

Da regjeringen vedtok at NOSIP-standarden skulle legges til grunn i staten. Norsk Open Systems Interconnection Profil var et viktig element i arbeidet med «elektronisk datautveksling» (EDU, engelsk: EDI) før Internett ble allment tilgjengelig.

13 Se forskrift av 15. desember nr 8962 punkt 6.1.1 og 6.1.5.

14 Se fvl §§ 16, 27 og 32, og efvf §§ 8 – 11.

15 Se forskrift av 2. februar 2001 nr 103.

16 Se lov om ligningsforvaltning av 13. juni 1980 nr 24.

17 Lov av 15. juni 2001 nr 8.

signaturer.[18] På lignende måte har eForvaltningsforskriften bestemmelser som skal bidra til sikker elektronisk kommunikasjon og dermed til at slike kommunikasjonsmåter får den tillit i befolkningen at de faktisk blir brukt.[19] Personopplysningsloven ses av mange primært som et hinder for å behandle personopplysninger, men representerer i minst like stor grad regler som skal sikre at elektronisk behandling av slike opplysninger skjer på en sikker måte. Således kan kravene til informasjonssikkerhet sies å borge for tillit og bidra til at folk faktisk tar i bruk elektroniske kommunikasjonsmidler i sin samhandling med forvaltningen.[20] Jeg vil likevel føye til at slik tilrettelegging snarere kan ses på som *hindring* dersom kravene er vanskelige og/eller dyre å gjennomføre og dermed kan komme i veien for bruk av teknologien. Jeg viser i denne sammenheng til det generelle problemet med å klassifisere rettsregler som enten hindring eller muliggjører, jf. avsnitt 2.1.

For det fjerde kan det i lover og forskrifter etablere materielle plikter og rettigheter på måter som muliggjør og stimulerer til utvikling og bruk av elektroniske løsninger i offentlig forvaltning. Det er sjelden med så åpne politiske debatter der det argumenteres utilslørt med hensynet til teknologi og administrasjon, som da Stortinget diskuterte innføring av pensjonspoeng for omsorgsarbeid i folketrygdloven. Pensjonspoeng ble ansett å være lite problematisk i forhold til omsorg for mindreårige barn fordi en her kunne gjøre bruk av barnetrygdregisteret. I loven ble det eksplisitt fastsatt at mottaker var «den som mottar barnetrygd for barnet etter barnetrygdloven» noe som gjorde at barnetrygdregisteret skulle brukes i administrasjonen av ordningen.[21] Mangel på lignende register som viste hvem som hadde omsorg for syke og eldre personer ble imidlertid brukt som argument *mot* at denne delen av folketrygdreformen ble gjennomført.[22] I først nevnte tilfellet var lovreformen stimulans til å etablere en IKT-basert løsning, i sist nevnte tilfelle var manglende mulighet til å gjøre bruk av IKT på en rasjonell måte et argument mot å gjennomføre lovendringen.[23]

Både opphavsrettigheter og bestemmelser vedrørende arbeidsmiljø kan muligens sies å være muliggjørende for utvikling av eForvaltningsløsninger. Argumentet er at de bidrar til å unngå, dempe og/eller løse konflikter som ellers

18 Se lovens § 6.
19 Se forskriftens kapitler 3 – 6.
20 Se personopplysningsloven § 13 og personopplysningsforskriftens kapittel 2.
21 Forskriften åpner for at krav kan fremsettes om at andre personer enn de som mottar barnetrygd kan tildeles pensjonspoeng.
22 Se særlig Innst. S. Nr . 200 (1988–89), s 33–34, Ot.prp. nr 77 (1989–90) og Innst. O. nr. 11 (1990–91), s. 9.
23 Til slutt ble resultatet imidlertid at begge grupper fikk tilleggspensjon. Se folketrygdloven § 3–16 med tilhørende forskrifter.

kunne hindret utvikling og/eller bruk av nye systemløsninger. På arbeidsplasser vil arbeidsgivers plikt til å involvere de ansatte i viktige endringsprosesser kunne gi høy grad av aksept for nye IKT-baserte arbeidsmåter.[24] En lignende positiv effekt kan bestemmelser som klargjør økonomiske rettigheter tenkes å ha. Forvaltningsledelsen og ansatte personer i forvaltningen som utvikler IKT-løsninger vil for eksempel komme inn under bestemmelsene i åndsverkloven om opphavsrett til datamaskinprogrammer (§ 39g) og enerett til eksemplarfremstilling og tilgjengeliggjøring av visse databaser mv. (§ 43). Med lovreguleringen reduseres trolig muligheten for at arbeidet rammes av uenighet.

3 Regelverk som stiller krav til selve systemutviklingsprosessen

I dette avsnittet gjennomgår jeg rettsregler som er relevante for prosessen med å utvikle eForvaltningsløsninger, herunder å transformere rettsregler som er formulert i vanlig norsk til rettsregler uttrykt i datamaskinprogrammer. Utvikling av beslutnings(støtte)systemer innebærer transformering[25] som kan muliggjøre alt fra helt begrenset til meget omfattende automatisering av rettsanvendelsen. Derfor må utgangspunktet være at det i ethvert slikt systemutviklingsarbeid må forventes å skje en *rettslig beslutningsprosess* der en tar stilling til hvorledes rettsregler skal fortolkes og anvendes av datamaskinsystemet. Valgene som blir truffet gjennom systemering, programmering mv. virker direkte inn på folks rettigheter og plikter.

Erkjennelsen av at systemutvikling innebærer å ta stilling til rettsspørsmål, gjør det nærliggende å spørre om det gjelder egne saksbehandlingsregler for slike arbeider, og i hvilken grad de som forestår utviklingsarbeidet står fritt i å velge modeller og metoder mv. for arbeidet. I andre rettslige beslutningsprosesser er det i høy grad saksbehandlingsregler som må følges. Avgjørelse av enkeltsaker skal for eksempel følge regler i forvaltningsloven,[26] og samme lov har også egne regler om utferdigelse av forskrifter. Grunnloven og Stortingets forretningsorden inneholder saksbehandlingsregler for lover,[27] og Utredningsinstruksen inneholder flere supplerende saksbehandlingsregler som kommer til anvendelse på Regjeringens behandling av forslag til lover

24 Se for eksempel arbeidsmiljøloven § 4–2 tredje ledd. Rett til brukermedvirkning kan være utdypet i avtaleverket og er uansett i samsvar med norsk systemutviklingstradisjon.

25 Hva slik transformering mer konkret innebærer får vente til neste avsnitt.

26 Kapitlene IV-VI får bare anvendelse i saker som gjelder enkeltvedtak, og bestemmelsene i kapittel VII bare i saker som gjelder forskrifter, mens bestemmelsene i kapittel II og III har generell anvendelse.

27 Se Grunnloven; særlig §§ 76 – 79 (jf. § 75 bokstav a) ,og Stortingets forretningsorden; f.eks. §§12, 28–31, 33, 48 og 58.

og forskrifter.[28] Når det imidlertid gjelder rettslige beslutningsprosesser vedrørende utvikling av IKT-baserte systemer i forvaltningen (jf. fagsystemer, beslutningssystemer, saksbehandlingssystemer mv.) gjelder det intet allment og samlet regelverk, og generelt er det kun få regler som direkte kommer til anvendelse. Dette betyr likevel ikke at slik systemutvikling skjer i et «rettstomt rom», og i det følgende skal jeg kort gjøre rede for hvorledes jussen har betydning for slikt utviklingsarbeid.

Et sikkert utgangspunkt er at alle bestemmelser i forvaltningsloven som ikke er spesielt knyttet til enkeltvedtak og forskrifter, gjelder for systemutvikling i offentlige forvaltningsorganer så langt bestemmelsene passer.[29] Dette betyr i alle fall at bestemmelser om habilitet, veiledningsplikt og taushetsplikt er aktuelle, se lovens kapitler II og III. Habilitetsbestemmelsene kan for eksempel få betydning i forhold til tildeling av kontrakter om kjøp av varer og tjenester, herunder outsourcing. Taushetsplikt under selve utviklingsarbeidet kan mest praktisk tenkes å gjelde «tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.»[30] Dersom forvaltningsorganet får tilgang til spesielle IKT-verktøy og systemutviklingsmetoder som et innleid konsulentfirma gjør bruk av, kan det for eksempel tenkes å gjelde taushetsplikt for dette.[31]

Forvaltningens alminnelige veiledningsplikt (fvl § 11) skal sette parter og andre interesserte i stand til å vareta sine interesser i bestemte saker på best mulig måte. Et planlagt eller pågående systemutviklingsarbeid kan trolig ses som en «sak» i denne sammenhengen. Dersom for eksempel berørte interesseorganisasjoner ønsker veiledning om betydningen av det pågående arbeidet for sine medlemmer, plikter vedkommende forvaltningsorgan derfor å veilede om dette. En aktuell situasjon er eksempelvis at Pensjonistforbundet henvender seg med spørsmål og bekymring vedrørende brukervennligheten i det pensjonsberegningssystemet som NAV utvikler. Omfanget av veiledningen må tilpasses forvaltningsorganets situasjon og kapasitet og det vil derfor sjelden være tale om plikt til dyptpløyende gjennomganger.

28 Se særlig Utredningsinstruksen, http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20000218–0108.html.

29 Flere bestemmelser er knyttet til eksistensen av en «part» (jf. § 2 bokstav e), og hvem som er part i ulike sammenhenger i et systemutviklingsarbeid kan konkret være vanskelig å ta stilling til.

30 Se henholdsvis fvl § 13 første ledd nr 1 og 2.

31 I praksis vil imidlertid forventningen være at firmaer selv betinger seg taushet om slike forhold.

De avgjørelser som treffes i et systemutviklingsarbeid og som har et klart rettslige innhold («rettslige systemavgjørelser», se avsnitt 3) *ligner på* «enkeltvedtak» og «forskrift» som er regulert i forvaltningsloven men må likevel antas å ikke komme direkte inn under disse bestemmelsene.[32] Forvaltningslovens kapitler IV – VII om varsling, saksforberedelse, begrunnelse, klage, høring og kunngjøring mv., gjelder altså i utgangspunktet ikke. Disse saksbehandlingsreglene er imidlertid utslag av allmenne forvaltningsrettslige prinsipper, og er derfor generelt relevante, også i forhold til den saksbehandlingen som leder fram til fastsettelse av det rettslige innholdet av forvaltningens beslutningssystemer mv. Dette betyr på den ene side at enkeltbestemmelsene i kapitlene IV – VII kan gi en viss veiledning. Således gir for eksempel fvl § 17 om utredningsplikt holdepunkter for å hevde at forvaltningsorganet må utrede spørsmål om lovtolkning mv. så godt som mulig før vedkommende rettsregel fastlegges, programmeres og iverksettes. Videre gir § 25 om begrunnelse holdepunkter for å kreve at forvaltningsorganet alltid bør kunne begrunne slike valg vedrørende rettsanvendelsen.[33]

På den annen side betyr eksistensen og relevansen av allmenne forvaltningsrettslige prinsipper at det ikke bare er forvaltningslovens utslag av prinsippene som kan gi veiledning for rettslige deler av systemutviklingen. I tillegg kan det utledes krav som på selvstendig måte er forankret i prinsippet. Slik kan prinsippet om forsvarlig saksbehandling tenkes å begrunne fremgangsmåter som ikke har noen parallell i bestemmelsene om enkeltvedtak og forskrifter. Hensynet til forsvarlig saksbehandling og ivaretakelse av rettssikkerhet kan for eksempel begrunne skriving av forklarende «stjernetekst» (kommentarer) i programkoden på en måte som legger til rette for legalitetskontroll. En kan imidlertid neppe på grunnlag av prinsippene formulere noen faste krav til fremgangsmåter, men må i stedet foreta en konkret vurdering av hvert systemutviklingsarbeid.

Arbeidsmiljøloven § 4–2 stiller krav som har direkte betydning for utvikling og bruk av informasjonssystemer. For eksisterende systemer stilles det krav om løpende informasjon til arbeidstakerne og deres tillitsvalgte, om opplæring og utforming av arbeidssituasjon.[34] Bestemmelsen regulerer også omstillingsprosesser som medfører endring av betydning for arbeidstakernes arbeidssituasjon (tredje ledd). I slike tilfelle skal arbeidsgiver sørge for den informasjon, medvirkning og kompetanseutvikling som er nødvendig for å ivareta lovens krav til et fullt forsvarlig arbeidsmiljø. Arbeidsmiljøet omfatter

32 Se nærmere om dette i neste avsnitt.

33 Se personopplysningsloven § 22 som i enkelte tilfelle direkte gir samme resultat.

34 Se aml § 4–2 første og annet ledd. Bestemmelsen gjelder ikke bare informasjonssystemer men ethvert system «som nyttes ved planlegging og gjennomføring av arbeidet».

både det psykososiale og det fysiske arbeidsmiljøet. Nye systemløsninger i offentlig forvaltning og endringer av eksisterende løsninger vil lett innebære at denne bestemmelsen kommer til anvendelse, for eksempel fordi systemløsningen gir nye krav til kompetanse, innebærer at arbeidsoppgaver av betydning faller bort, at arbeidstakere blir overvåket for eksempel ved hjelp av ulike typer logging mv.

I tillegg til den generelle reguleringen kommer særlige bestemmelser i avtaleverket, og i Hovedavtalen i staten gjelder § 14 spesielt for anskaffelse, utvikling, herunder betydelige endringer av informasjons- og kommunikasjonsteknologi. I slike tilfelle skal ledelsen og tillitsvalgte avtale (dvs bli enige om) hvordan de tilsatte skal medvirke og hvordan deres erfaringer skal bli tatt vare på i utviklingsarbeidet. Det gjelder med andre ord bestemmelser om brukermedvirkning i utviklingsarbeidet, samtidig som det er opp til partene selv å bestemme hvorledes dette skal skje. For øvrig gjelder hovedavtalens generelle system om informasjon, drøfting og forhandlinger, jf. avtalens §§ 11 – 13. Jeg kommer ikke nærmere inn på forståelsen av disse bestemmelsene her, men nøyer meg med å fremheve at de kan innebære en rett til drøfting (meningsutveksling) og – i noen tilfelle – forhandling (enighet) også i spørsmål om omorganisering mv. som skjer i tilknytning til anskaffelse/endring av IKT-systemer.

I tillegg til at lov, forskrift og avtaler kan ha betydning for systemutviklingen, kan det være gitt bestemmelser *internt* i forvaltningen som gjelder for systemutviklingsarbeidet. For det første kan det være gitt føringer i form av instrukser og retningslinjer i tilknytning til det enkelte utviklingsprosjektet, for eksempel i mandatet til prosjektgruppen. Det kan også være gitt generelle instrukser/retningslinjer på etatsnivå. Her skal jeg imidlertid nøye meg med en kortfattet diskusjon vedrørende relevansen av Utredningsinstruksen, gitt ved kongelig resolusjon[35] og med gyldighet for hele statsforvaltningen. Bestemmelsene tar særlig sikte på å få klarlagt økonomiske, administrative og andre vesentlige konsekvenser av «reformer og tiltak». Ikke enhver saksbehandling som foregår i offentlig forvaltning skal følge prosedyrene i Utredningsinstruksen. Hvorvidt instruksen skal følges, beror på en konkret vurdering av sakens karakter.[36]

Systemutviklingsarbeider er ikke eksplisitt nevnt i instruksen eller den tilhørende veiledningen fra FAD, men kan etter omstendighetene likevel omfattes. Forutsetningen er trolig at arbeidet kan eller vil ha vesentlige konsekvenser. Det er med andre ord ikke nødvendig at selve utviklingsarbeidet i seg selv skal være omfattende. Avgjørende er ikke omfang med hvor vesentlige konsekvensene er

35 Se kgl. res. av 18. februar 2000, revidert ved kgl. res. av 24. juni 2005.
36 Se FADs veiledning, punkt 1.3.

for vedkommende forvaltningsorgan, andre deler av forvaltningen og samfunnet for øvrig. Personvern, enklere regelverk og enklere forvaltning er særlig nevnt i FADs veileder som noen typer aktuelle konsekvenser, men det fremgår av dokumentet at dette kun er en eksemplifisering.[37]

Dersom Utredningsinstruksen kommer til anvendelse på et systemutviklingsarbeid vil det gjelde regler vedrørende krav til konsekvensutredning, foreleggelsesplikt og alminnelig høring. Her skal jeg bare kort kommentere hvert av disse tre hovedpunktene. Konsekvensutredning er både aktuelt i tilknytning til utforming av oppdrag/mandat til en prosjekt-/utredningsgruppe (forhåndsvurdering) og som del av de vurderinger og løsningsforslag som slike grupper fremlegger. Forhåndsvurderingen av konsekvenser skal på visse vilkår forelegges berørte departementer. Dette innebærer bl.a. at systemutviklingsprosjekter som antas å kunne medføre vesentlige administrative og/eller organisatoriske endringer i statsforvaltningen skal forelegges Fornyings- og administrasjonsdepartementet. Utviklingsprosjekter som innebærer felles systemløsninger mellom forvaltningsorganer (jf. Min Side og AltInn), kan etter dette antas å komme inn under plikten til foreleggelse.[38]

Analyse og vurdering av økonomiske og administrative konsekvenser skal alltid inngå i selve utredningsarbeidet, herunder arbeid som gjelder systemutvikling og som kommer inn under Utredningsinstruksen. I tillegg skal saken vurderes i forhold til alle overordnede eller generelle hensyn som kan ha betydning ved vurderingen av om forslaget skal iverksettes. Brukervennlighet, personvern, informasjonssikkerhet og rettssikkerhet vil med andre ord kunne være aktuelle vurderingstemaer, men det eksisterer ingen obligatorisk liste over slike andre vurderinger.[39] Foreleggelse for departementer kan også være aktuelt etter at en utredning er ferdig men før alminnelig høring gjennomføres. Instruksen inneholder flere unntak fra regelen om høring som kan være aktuell for systemutviklingsprosjekter, bl.a. at høring ikke vil være praktisk gjennomførlig, se punkt 5.4 bokstav a. Instruksen skal imidlertid trolig forstås slik at foreleggelse etter utredningen er klar kan være aktuell selv om alminnelig høring ikke gjennomføres. Vilkåret er uansett at konsekvensutredningen viser at saken kan medføre vesentlige økonomiske, administrative eller andre vesentlige konsekvenser på andre departementers ansvarsområder eller berører disse i vesentlig grad på annen måte, jf. punkt 4.3 i instruksen.

Utredningsinstruksens utgangspunkt er som nevnt at saker som er ferdig utredet skal sendes på alminnelig høring til alle berørte offentlige og private

37 Se FADs veiledning, punkt 11.3.
38 Se instruksens punkt 4.2.1, henholdsvis punktene b og c.
39 Jf. Utredningsinstruksens punkter 2.3.1 og 2.3.2.

institusjoner og organisasjoner.[40] Unntak kan bl.a. gjøres når høring ikke er praktisk mulig og når det er åpenbart unødvendig. Dersom det gjøres unntak bør synspunkter innhentes fra berørte på andre måter. Selv om et forslag til systemløsning kan være umulig å sende på høring i vanlig forstand, kan instruksen forstås slik at dialogen med berørte aktører skal sikres på annen måte, for eksempel ved å sende ut et dokument som redegjør for hovedpunktene i forslaget, arrangere høringsmøte eller på annen måte.

4 Regelverk som innhold i forvaltningens IKT-systemer

Beslutnings- og beslutningsstøttesystemer kan helt eller delvis sette forvaltningsorganene i stand til å automatisere rettsanvendelsen i enkeltsaker, se eksempler på dette i kapitlene 5 – 7 (ovenfor). For at dette skal kunne skje, må det gjennomføres en fortolkning av relevante rettskilder innenfor det aktuelle forvaltningsområdet. Utgangspunktet vil normalt være regelverk i form av særlovgivning som fortolkes i lys av øvrige rettskilder.[41] I fylkeskommunenes beslutningssystemer vedrørende inntak til videregående opplæring, ligger det f.eks. en representasjon av inntaksreglene, jf. kapittel 6 i forskrift til opplæringslova.[42] Slike systemløsninger har med andre ord et innhold som gir generelle anvisninger på hvorledes rettsspørsmål innen det aktuelle rettsområdet skal løses. I beslutningssystemer,[43] dvs der automatiseringsgraden er høy, vil slike generelle rettslige avgjørelser foreligge i høyt antall og stor detalj.

4.1 Fra saksdrevet til systemdrevet fortolkning

Desto mer ekstensive og intensive forvaltningens beslutningssystemer blir, desto flere rettsspørsmål vil bli løftet fra et manuelt/individuelt nivå (i tilknytning til hver sak), opp til et automatisert/generelt nivå (i tilknytning til det aktuelle beslutningssystemet). Vi beveger oss med andre ord fra en situasjon der rettskildene blir fortolket og anvendt fordi konkrete saker gjør det nødvendig («saksdrevet fortolkning»), til en situasjon der rettskildene blir fortolket og

40 Unntak gjelder for proposisjoner og meldinger til Stortinget som behandles i tråd med instruksens kapittel 6.

41 Også generell forvaltningslovgivning kan tenkes å inngå i beslutningssystemer, men i Norge skjer dette svært sjelden.

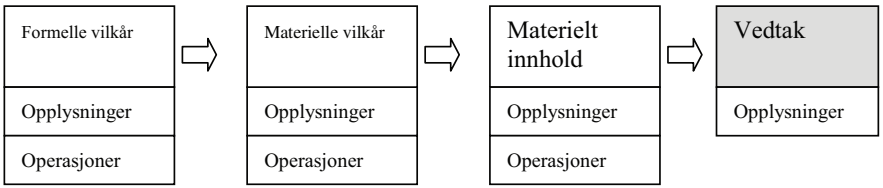
42 Se lov av 17. juni 1998 nr.61 og forskrift av 28.juni 1999 nr. 722.

43 Jf. beslutningsstøttesystemer.

nedfelt i programkode fordi etableringen av beslutningssystemet gjør det påkrevet («systemdrevet fortolkning»).[44]

Systemdrevet fortolkning innebærer i tillegg en forskyvning i tid: Årsaken er at alle rettsspørsmål som skal inngå i systemløsningen vil bli løst før de er aktualiserte av konkrete saker. Dette ligner slike instrukser om rettsanvendelsen som en i mange etater nedfeller i «rundskriv». Fortolkninger nedfelt i programkode representerer imidlertid en mer bastant og omfattende form for forhåndsavgjørelse av rettsanvendelsesspørsmål, jf. nedenfor.

Systemdrevet fortolkning innebærer en spesiell tilnærming til rettskildene. Utfordringen er å spesifisere en prosedyre med detaljerte anvisning på hvorledes hver sakskategori skal bli behandlet for å nå frem til et rettsriktig resultat. I figur 2 er dette illustrert ved hjelp av tre generelle regelkategorier: Først må formelle krav til saksbehandlingen kartlegges (rett myndighet, krav til overholdelse av frister, krav til bruk av skjemaer mv.). Deretter må de materielle vilkårene for vedtak undersøkes (f. eks. vilkår for skatteplikt, vilkår for rett til opptak til videregående skole mv.); og til slutt må de rettsreglene som er avgjørende for innholdet av vedtaket kartlegges og fortolkes (regler for utligning av skatt, regler for prioritering av søkere til videregående skole mv.). Til hver type rettsspørsmål må det samles inn og prosesseres noen opplysninger.



Figur 2: Grunnleggende systematikk for en systemdrevet fortolkning

Siden målet er å sette datamaskinen i stand til å anvende rettsregler, er utfordringen dessuten å kunne fortolke rettskildene på en måte som samsvarer med egenskaper ved informasjonsteknologien. Dette gir flere viktige effekter: For det første må vi på forhånd angi alle lovlige opplysningstyper som kan godtas som beslutningsgrunnlag. Desto høyere automatiseringsgrad, desto flere opplysningstyper må formaliseres, dvs. defineres ved hjelp av tillatte koder, verdiområder mv. Opplysningene kan herunder defineres i overensstemmelse med opplysningstyper som er maskinelt tilgjengelige, noe som gjør det mulig med

44 Se nærmere om dette i Dag Wiese Schartum, Utvikling av beslutningssystemer -fra lovtekst til programkode, tilgjengelig fra http://www.afin.uio.no/forskning/notater/utvikling_av_beslutningssystemer.pdf.

automatisk innhenting av saksopplysninger fra interne og eksterne databaser. Innenfor de definerte rammene kan slike fremgangsmåter gi en presis og fast beskrivelse av enkeltsaker. Formalisering av opplysningstyper begrenser imidlertid mulighetene for å beskrive særegenheter ved enkeltsaker. Det er derfor fare for en «firkantet» rettsanvendelse som oppleves som urettferdig.

Når oppgaven er å utvikle et beslutningssystem, er det også nødvendig å ta stilling til hva som skal skje med saksopplysningene for å nå frem til korrekte vedtak. Vi må med andre ord lete etter dynamiske elementer i rettskildene som lar seg automatisere. Siden datamaskinen er en «regne- og logikkmaskin», blir spørsmålet om rettsreglene kan forstås på måter som lar seg uttrykke ved hjelp av aritmetiske og logiske operasjoner.[45] Resultatet av en slik fortolkning blir konkrete angivelser av hvilke vilkårsprøvinger og beregninger som må utføres for å få rettsriktige vedtak. Samtidig som behandlingsreglene blir konkret angitt, kan dette innebære en avgrensing av hvilke behandlingsregler som kan legges til grunn, jf. straks nedenfor.

Når en skal vurdere det rettslige innholdet i beslutningssystemer, er et sentralt spørsmål om løsningene i systemet vil bli lagt til grunn for all behandling av enkeltsaker med den konsekvens at systemet faktisk bestemmer rettsanvendelsen, eller om det kan gjøres avvik fra løsningene? Spørsmålet er med andre ord om innholdet i systemet «generelt er bestemmende for» «rettigheter eller plikter til en eller flere bestemte personer», jf. definisjonen av enkeltvedtak.[46] Problemet med beslutningssystemer er at det kan være usikkerhet på dette helt sentrale punktet. Situasjonen kan være at reglene i systemet følges automatisk og i er bestemmende i det store flertallet av saker, mens det innen spesielle sakstyper kan skje avvik. Årsaker til avvik kan være at det er feil eller ufullstendigheter i systemet. Det kan også være at en bevisst har valgt å utvikle et system som ikke gir en fullstendig representasjon av gjeldende rett, og at en derfor må behandle visse sakstyper manuelt. Det dominerende bildet vil imidlertid – uansett – være at de regler som er lagt til grunn i programkoden følges og derfor i praksis får bestemmende innvirkning på nesten alle saker som behandles i systemet.

Etter min mening bør det stilles krav til en nærmere klargjøring av hvilken rettslig karakter beslutnings(støtte)systemer har. Forvaltningsorganer bør med andre ord ta stilling til hvilke deler av systemet som skal legges til grunn uten forbehold, og hvilke deler av systemet som (eventuelt) kan/skal ses på som veiledende. Denne kunnskapen må dessuten kommuniseres til alle parter som får

45 Dvs om rettsreglene kan uttrykkes ved hjelp av operatorer som for eksempel +, –, and, or osv.. eller uttrykk av typen if .. then else osv., eller som kombinasjoner av disse.

46 Se forvaltningsloven § 2 bokstav b, jf. bokstav a.

sin sak behandlet, slik at de kan bli klar over hva forvaltningsorganet mener kan være gjenstand for konkret argumentasjon.

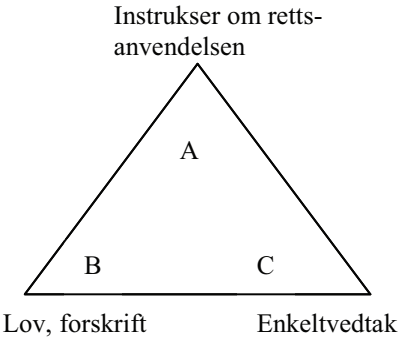
Eksistensen av lover, forskrifter mv. innebærer en plikt for personer i forvaltningsorganet til å utføre saksbehandlingen på en bestemt måte. Som for all menneskelig adferd er det imidlertid en usikkerhet mht graden av faktisk etterlevelse. Ved manuell saksbehandling kan rettsanvendelsen bli uriktig fordi saksbehandler mangler kunnskap, slurver e.l. I eForvaltningen må etterlevelsen primært skje på «systemnivå», dvs i tilknytning til utviklingen av beslutningssystemet mv. I stedet for kontinuerlig å sikre riktig rettsanvendelse blant mange saksbehandlere, blir utfordringen å sikre riktig rettsanvendelse hos den (relativt) lille gruppen personer som utvikler selve systemløsningen. Og har man først et rettsriktig system, vil det fortsatt være korrekt inntil det skjer endringer i rettskildebildet. Rettsreglene blir i så fall ikke bare tekst, men «handlinger» som datamaskinprogrammet utfører på alle enkeltsaker av et visst slag. Det som utvikles innenfor rammene av eForvaltningsprosjekter er med andre ord ikke (bare) instrukser og henstillinger til personer som er uttrykt i naturlig språk der «den menneskelige faktor» skaper usikkerhet om etterlevelse og resultat. eForvaltningen innebærer at det i stor grad blir gitt entydige instrukser til maskiner som derfor blir konsekvent utført i alle enkeltsaker som behandles i systemet.

4.2 Rettslige systemavgjørelser

Flere elementer i den foregående gjennomgangen av arbeidet med å fastlegge det rettslige innholdet av beslutningssystemer i eForvaltningen, peker i retning av nærmere rettslig regulering av denne utviklingsprosessen. Avslutningsvis i dette avsnittet vil jeg nøye meg med å peke på mer grunnleggende problemer av forvaltningsrettslig og demokratisk karakter.

Det er etter min mening avgjørende å ta stilling til om en i forvaltningsretten skal forholde seg aktivt til de rettslige elementene som inngår i utviklingen av beslutningssystemer og andre eForvaltningsløsninger eller ikke. Alternativt kan en velge kun å forholde seg til de enkeltvedtak som treffes ved hjelp av disse systemløsningene, med andre ord bare forholde seg til *virkningene* av systemet. Etter min mening er det nødvendig å velge begge tilnærminger, dvs både forholde seg til systemutviklingen og til bruken av systemene. Årsaken er primært at det er uaktuelt for de fleste å kontrollere selve datamaskinprogrammet, og at en reell legalitetskontroll av konkrete enkeltsaker vil være begrenset til et meget lite antall saker. Derfor må legaliteten både sikres gjennom tilblivelsen og bruken av eForvaltningens systemløsninger.

I sin tid ble det diskutert om datamaskinprogrammer med rettslige innhold kunne ses som «forskrift» i tråd med definisjonen i fvl § 2 bokstav c, jf. bokstav a.[47] Konklusjonen syntes å være at det ikke i slike tilfelle forelå «forskrift», men at det *lignet*. Tilsvarende kan det hevdes at beslutninger om innholdet i slik programkode ligner tradisjonelle instrukser om rettsanvendelsen. En viktig forskjell er imidlertid at de er instrukser til maskiner og ikke mennesker, og at de utføres automatisk. Det kan videre hevdes at slik programkode kan determinere resultater i enkeltsaker – særlig dersom programmet både angir maskinelt tilgjengelige opplysningstyper i saken og behandlingsreglene for disse.[48] Selv om koden ikke inneholder enkeltvedtak, kan vedtakene i slike tilfelle sies å ligge implisitt i koden.



Figur 3:Beslutningstyper i tilknytning til utvikling av rettslige beslutningssystemer

Fastsettelse av det rettslige innholdet av beslutningssystemer mv. i forvaltningen kan med andre ord sies å ligne flere tradisjonelle rettslige beslutningstyper, men er samtidig *forskjellige* fra disse. I figur 3 har jeg forsøkt å illustrere dette poenget ved å angi tre «beslutningsposisjoner» (A, B, C) knyttet til utvikling av slike systemer. Hver av posisjonene markerer beslutninger som treffes som ledd i utvikling av beslutningssystemer i forvaltningen, og plasseringen i forhold til tradisjonelle beslutningstyper (forskrift, instruks, enkeltvedtak), markerer likhet med disse. Avgjørelsene i A, B og C betegner jeg *rettslige systemavgjørelser*.[49] Poenget er at forvaltningen i stor grad kan velge hvilke egenskaper slike systemavgjørelser skal ha: De kan primært treffe avgjørelser

47 Se Eckhoff (1992, s 565) med videre henvisninger.

48 Men verdiene av hver opplysningstype kan forandre seg, og innholdet av enkeltvedtaket er uansett ikke synlig før programmet er anvendt.

49 Se Schartum (2000).

som kan fravikes, men som normalt skal følges, jf. A i figuren. De kan også treffe avgjørelser som de ønsker å legge til grunn i alle saker, men som i liten grad determinerer den enkelte sak fordi opplysningene som skal utgjøre det faktiske beslutningsgrunnlaget i den enkelte sak i liten grad er fastlagt, jf. B i figuren. Punktet «C» markerer rettslige systemavgjørelser som forvaltningsorganet legger til grunn i alle saker, og som også definerer det faktiske beslutningsgrunnlaget. I dette siste tilfellet vil systemet både angi maskinlesbare kilder som opplysningene i saken skal hentes fra, samt alle regler for behandling av disse opplysningene som leder frem til enkeltvedtak. Vedtaket ligger da «bare et tastetrykk unna».

Jeg vil sterkt fremheve betydningen av å beskrive deler av systemutviklingsarbeidet som en *rettslig beslutningsprosess*. Samtidig er det viktig å understreke at en slik prosess kan lede til resultater som bør vurderes på noe ulike måter. Tilfellene i A er de som rettslig sett har svakest innvirkning på enkeltvedtak, mens tilfellene i C har svært stor innvirkning. Et sentralt spørsmål er i hvilken grad det bør stilles krav til de rettslige beslutningsprosessene som inngår i utvikling av beslutningssystemer. Videre er spørsmålet i hvilken grad det bør gis særskilte rettssikkerhetsgarantier knyttet til bruk av beslutningssystemer. I begge tilfelle er det klart sterkere grunn til å regulere tilfellene C (og B) enn i A. Spørsmålene blir ikke drøftet nærmere her.

5 Virkninger av systemutvikling på regelverksutvikling

Allerede i 1977 skrev Jon Bing om *automatiseringsvennlig lovgivning* dvs lovgivning som er skrevet på en måte som legger til rette for enkel transformering fra lovtekst i vanlig norsk til lovtekst uttrykt som programkode. Noen som hører slike uttrykk kan grøsse over muligheten for at lovvedtak, dvs. avgjørelser i selve kjernen i folkestyret, skal kunne påvirkes av teknologiske krav. I begrepet automatiseringsvennlig lovgivning kan det imidlertid ligge flere muligheter og ikke alle er like kontroversielle.

5.1 Håndtering av skjønn i beslutningssystemer

For mange vil spørsmål vedrørende utøvelse av skjønn stå sentralt når lovgivning og automatisering skal diskuteres. Et skjønn innebærer en type frihet for beslutningsfatteren som innebærer at det prinsipielt sett ikke er mulig å formalisere beslutningen. Det er med andre ord ikke mulig på forhånd uttømmende å fastsette hva som skal være relevant for skjønnsutøvelsen og hvilken vekt hvert moment skal ha. Gjør man det har man prinsipielt sett fjernet skjønnet, fordi skjønnet grunnleggende er åpent. Således kan det for eksempel ikke på

forhånd angis på faste måter hva som i fremtiden skal anses å være «rimelig», «tilfredsstillende» eller «forsvarlig» når slike uttrykk inngår i en rettsregel. Det skal alltid skje en konkret vurdering.

Siden skjønn ikke lar seg automatisere kan man hevde at en ved å fjerne skjønnet kan gjøre rettsreglene automatiseringsvennlige. Det kan for eksempel tenkes at uttrykk som «tilfredsstillende» osv erstattes av et sett med andre, faste vilkår som i kombinasjon forutsettes å resultere i at kriteriet «tilfredsstillende» er oppfylt. Desto flere slike faste kriterier som trekkes inn og desto hyppigere disse kriteriene blir oppdatert, desto større er sannsynligheten for at resultatet *nærmer seg* det som ville blitt resultatet av en skjønnsutøvelse.

Selv om en prinsipielt ikke kan erstatte skjønn med faste kriterier, kan det være at resultatet av å behandle faste kriterier i stedet uansett blir bedre enn med skjønnsutøvelse. Gitt tids- og arbeidspress for den som skal utøve skjønnet, begrenset kunnskap om relevante forhold mv., kan det være at skjønnsutøvelsen i realiteten blir en forholdsvis overflatisk og intuitiv vurdering, i verste fall tilfeldig. For å unngå at det skal bli tilfellet kan en utarbeide huskeliste for skjønnsutøveren, dvs angi lister av momenter som det kan være relevant å legge vekt på.[50] Men i så fall står en i fare for at det er listen (og dermed faste kriterier) og ikke selve skjønnstemaet som styrer avgjørelsene. Derfor er det ikke sikkert at det virkelig går tapt så mange kvaliteter ved beslutninger dersom skjønnet forsvinner til fordel for flere faste kriterier.

Faste kriterier som grunnlag for å erstatte manuell skjønnsutøvelse med automatisert behandling vil imidlertid normalt kreve stor informasjonstilgang fra maskinlesbare kilder. Hvis «tilfredsstillende sikkerhet» skal erstattes må det for eksempel angis om ulike sikringstiltak er iverksatt eller ikke. For hvert tiltak kreves det informasjonstilgang. Å erstatte et skjønn med ti faste kriterier vil derfor kunne være dyrt. Derfor kan det skje at skjønnet ikke erstattes av mange faste kriterier men kun av noen få, og i så fall vil avgjørelsen bli langt mer «firkantet». Selv om faste kriterier i teorien kan gi en like nyansert behandling av enkeltsaker som ved manuell skjønnsutøvelse i en presset arbeidssituasjon, kan realiteten likevel bli motsatt. Det megetsigende svaret på spørsmålet om skjønn eller faste kriterier er best er med andre ord; «det kommer an på».

Selv om skjønn ikke lar seg formalisere, er det fullt mulig å integrere skjønnsutøvelse i en automatisert beslutningsprosess. Dette kan skje ved at *resultatet* av en skjønnsutøvelse registreres i beslutningssystemet og blir gjenstand for videre behandling. For eksempel registreres verdien «ja» eller «nei»

50 Eksempler på dette er beskrevet i Torstein Eckhoff og Hans Petter Graver: Regelstyring av lokale forvaltningsvedtak: praktisering av bygningsloven, Tano 1991.

som resultat av vurderingen av om noe er «forsvarlig», og denne verdien inngår i en videre automatisert behandling.

5.2 Formalisering av rettsreglene

Automatiseringsvennlig lovgivning handler om mer enn skjønn og faste kriterier. Et annet sentralt eksempel er at lovgivningen formuleres slik at de opplysningstypene som inngår i rettsreglene er slike som faktisk finnes i maskinlesbar form. Dersom det i jaktloven står «jeger» vil det være automatiseringsvennlig hvis dette begrepet var definert slik at det alltid samsvarer med personer oppført i jegerregisteret. Tilsvarende kunne en la «bosatt i riket» tilsvare alle de som var registrert i folkeregisteret (e.l.). Også slik formalisering vil kunne skape usikkerhet, for eksempel fordi de *reelle* forholdene avviker fra de som assosieres med definisjonene (f. eks. personen som er bosatt i riket er på reise i utlandet mesteparten av året). Rettferdighetsvurderingen, særlig i forhold til formålet med den rettslige reguleringen, kan derfor være avgjørende for om denne type tilpasning til automatisering er akseptabelt eller ikke.

Den neste formen for automatiseringsvennlighet jeg vil nevne gjelder tydeliggjøring av de logiske og aritmetiske operasjoner som rettsreglene beskriver. En lovtekst forutsetter for eksempel at en slutningsrekke skal utføres og beregninger foretas, for eksempel slik at slutningene danner grunnlag for hvilke beregninger som skal skje. Det stilles for eksempel opp vilkår for å kunne motta en ytelse, plikt til å betale skatt, for opptak til et universitetsstudium osv, og deretter beregnes trygd, skatt, studiepoeng mv. I så fall er det særlig viktig å ta stilling til i) hvilke vilkår som kan stilles, ii) om de er alternative eller kumulative mv. og iii) hvilken rekkefølge de skal utføres i. Med beregninger er det tilsvarende viktig å få klart frem hvilke aritmetiske operasjoner som skal utføres og nøyaktig på hvilke måter.

Når lover og andre rettskilder skal transformeres til programkode for helt eller delvis å automatisere rettsanvendelsen står de logiske og aritmetiske operasjoner som skal utføres sentralt. I tradisjonell lovgivning vil vilkårsstrukturer og beregningsmåter være uttrykt ved hjelp av vanlig norsk, noe som ikke alltid gir en tilstrekkelig presisjon og kan etterlate unødvendig tvil når bestemmelsene skal transformeres til programkode. Lovgivning kan derfor gjøres «automatiseringsvennlig» ved at en i større grad bruker ord og oppsett i lovtekstene som øker presisjonsnivået, for eksempel slik at en i oppregninger av vilkår tydeliggjøre om det er tale om OG, ELLER, IKKE osv og tilstrekkelig tydelig gjør bruk av matematiske operatorer for entydig å gi anvisning på hvilke regneoperasjoner som skal utføres.

Automatiseringsvennlig lovgivning kan med andre ord sies å spenne fra det å fjerne skjønnsutøvelse og formalisere beslutningsgrunnlag (noe som ofte er kontroversielt), til det å tydeliggjøre viktige innholdsmessige strukturer for derved å gjøre arbeidet med å fortolke og transformere bestemmelsene til programkode enklere.

Selv om man *ikke* velger å gjøre lov- og forskriftstekster mer automatiseringsvennlige kan det likevel være et poeng å gjøre bruk av formalisering som del av lov*forarbeidet*. Det kan med andre ord være nyttig for lovgiver å sette opp regnestykker som skal inkorporeres i en lovtekst som et formelt matematisk uttrykk før dette formuleres i vanlig norsk, og slike matematiske oppsett kan med fordel inngå i forarbeider som støtte ved den etterfølgende fortolkningen av lovbestemmelsene. Det kan også undersøkes om begreper som lovgiver ønsker å bruke allerede finnes i eksisterende relevant lovgivning og om tilhørende datadefinisjoner er brukbare. Selv om en ikke velger å gjøre felles bruk av et datasett vil slike undersøkelser kunne øke kunnskapsgrunnlaget og styrke begrunnelsen for de valgene en gjør. På tilsvarende måte kan det være lærerikt i lovforarbeidet å undersøke i hvilken grad faste kriterier kan uttrykke en ønsket løsning; om ikke annet for i forarbeidene å kunne angi hva som kan forventes å være viktige elementer i det skjønnet lovgiver i stedet gir anvisning på.

6 «Lovgivningsvennlig automatisering»: Systemutvikling som regelverksutvikling

Lovgivning er i utgangspunktet lite automatiseringsvennlig, det vil si det må ofte avklares en rekke tolkningsspørsmål som ledd i transformeringen fra lov til programkode, jf. forrige avsnitt. Av dette følger det blant annet at det som ledd i systemutviklingsarbeidet må skje omfattende analyser av de bestemmelser i lov og forskrift mv. som skal transformeres til programkode. Slike gjennomganger vil ikke sjelden avdekke at det er gjort mangelfullt lovgivningsarbeid. Begrepsbruken i lovteksten er for eksempel inkonsekvent, det kan være uklart hvordan en beregning skal skje, hva beslutningsgrunnlaget skal være, hvilke vilkår som må være oppfylt mv. Systemutviklingen vil gjøre det nødvendig å bringe klarhet i alle slike vesentlige spørsmål som berører programmering mv. Det vil derfor alltid foreligge en entydig løsningsbeskrivelse på de tolkningsspørsmål som lovbestemmelsene mv. reiser.

Det er selvsagt mulig bare å løse de tolkningsspørsmålene som mangelfullt lovgivningsarbeide skaper på best mulig måte og implementere disse uten å bry seg mer om vedkommende regelverk. I så fall kan det imidlertid oppstå stor avstand mellom det loven uttrykker rent språklig sett, og det som faktisk legges

til grunn i systemet. Hensynet til konsistens, sammenheng i rettssystemet og forutberegnelighet kan tilsi at en bruker analyseresultatene fra utviklingsarbeidet til også å utvikle regelverket. Det kan med andre ord være grunn til å pløye innsikter fra systemutviklingsarbeidet tilbake til lovteksten. Dette er selvsagt særlig aktuelt i tilfelle der analyseresultatene primært gjør det mulig å uttrykke det samme regelinnholdet på en lettere forståelig måte enn den aktuelle lovteksten uttrykker. For eksempel kan det klart uttrykkes i lovteksten at et vilkår er alternativt og på den måten å gjøre det unødvendig å lese forarbeider mv. for å bli sikker i spørsmålet; og man kan endre på klart umotivert og inkonsekvent begrepsbruk for på den måten lette forståelsen.

Oppretting av klare svakheter ved utforming av en lovtekst og endringer som primært er av lovteknisk (og ikke innholdsmessig) karakter, er relativt lite kontroversielt – selv om det ikke nødvendigvis er enkelt å gjennomføre. Det kan imidlertid være grunn til også å gjøre innholdsmessige endringer på bakgrunn av de analyser som skjer ved utvikling av systemløsninger som skal sette lovgivningen ut i livet. Undersøkelser viser for eksempel at det ved utvikling av beslutningssystemer kan være behov for flere/supplerende regler i forhold til de lovgiver har gitt.[51] Det kan også være at en formulerer regler som strengt tatt må sies å avvike fra det lovgiver har bestemt. Spørsmålet er om det i det hele tatt er akseptabelt at det eksisterer klare avvik mellom lovgivning og de reglene som faktisk legges til grunn i systemløsningene? Dersom en som del av systemutviklingsarbeidet mener det er behov for flere regler enn det som følger av rettskildene (lov, forskrift mv.) bør man i utgangspunktet bestandig kreve at slike nye regler alltid også kommer til uttrykk i lovteksten e.l. Tilsvarende er det meget problematisk å akseptere et regelinnhold i programkoden som klart avviker fra det som kan sies å følge av lovteksten mv.

7 Om forholdet mellom regelutvikling og organisasjonsutvikling

I dette avsnittet vil jeg kort komme inn på forholdet mellom regel- og organisasjonsutvikling når dette står i samband med utvikling og bruk av IKT. Situasjonen er med andre ord enten at IKT bevirker organisasjonsendring som igjen krever endringer i den rettslige reguleringen, eller at IKT foranlediger regelendring som igjen innebærer krav til endret organisering. Jeg vil her nøye meg med å gjennomgå to praktisk viktige situasjoner.

Et vesentlig aspekt ved IKT og særlig Internett-teknologi er at den legger til rette for å endre organiseringen av offentlig sektor og denne sektorens

51 Se om dette i Dag Wiese Schartum: En rettslig undersøkelse av tre edb-systemer i offentlig forvaltning, Tano 1989.

samhandling med aktører i privat sektor og befolkningen generelt. Det er for eksempel mulig å la den enkelte part i forvaltningssaker få et hovedansvar for behandlingen av egen sak ved å la parten bli direkte bruker av forvaltningens beslutningssystem. Når parten har avgjørende innvirkning på egen saksbehandling kan vi kalle denne organiseringen for «selvbetjent forvaltning».[52] Speditører kan for eksempel gjøre bruk av tolletatens system for deklarering av gods, elever kan gjøre direkte bruk av fylkeskommunens system for opptak til videregående skole osv. Poenget med selvbetjening er ikke at det kun er parten som har innflytelse, men at partens innflytelse er stor og vesentlig større enn dersom partene utfyller skjemaer som etterpå blir vurdert/kontrollert av saksbehandler før den blir maskinelt behandlet. I de tilfelle det er meningsfullt å bruke betegnelsen selvbetjening spiller ikke saksbehandlere noen avgjørende rolle (i hvert fall ikke i ordinær behandling); parten er langt på vei «sin egen saksbehandler». Teknologien kan også legge til rette for andre typer arbeidsdeling, men her holder meg til den selvbetjente forvaltningen.

Dersom forvaltningen velger en arbeidsdeling med klare elementer av selvbetjening kan dette åpenbart kreve behov for regelendringer. For eksempel kan det være behov for å supplere/presisere regler for identifisering og autentisering av parter som bruker systemet. Det kan også være behov for å regulere i hvilken grad og på hvilken måte parter skal ha krav på veiledning og assistanse når de behandler sin egen sak, avklare ansvaret for feil, forvaltningsmyndighetens adgang til å kontrollere parten, forutsetningene for og inneholdet av klage på vedtak som parten selv har forestått mv. Generelt må det antas at enhver vesentlig endring av organiseringen vedrørende arbeidet med å treffe enkeltvedtak aktualiserer behov for regelendring, spesielt når endringer skaper nye utfordringer for partenes rettssikkerhet og/eller personvern. Eksempelet selvbetjent forvaltning illustrerer at slike endringer kan oppleves som gradvise og «umerkelige». Vi kan hevde at folk «alltid» har fylt ut skjemaer selv og at det derfor knapt er grunn til regelendring bare fordi skjemaet i dag fylles ut på en skjerm! Slik likhet kan imidlertid være bedragersk fordi det samtidig kan ha skjedd endringer som innebærer at saksbehandlers konkrete vurdering av enkeltsaker har falt helt bort, forvaltningsmyndigheten kan ikke lett oppsøkes fordi det kan ha skjedd sentralisering eller regionalisering av forvaltningskontorene, regelverket kan ha blitt mer komplisert enn tidligere, horisontalt samarbeid mellom forvaltningsorganer kan gjøre det uklart hvilket organ som har ansvaret osv.

52 Se Dag Wiese Schartum: Den selvbetjente forvaltning. Om saksutredning ved behandling av enkeltsaker i masseforvaltningen.. Nordisk Administrativt Tidsskrift 1994 (1):32–47.

Som eksempel på hvorledes regelutvikling påvirker organisering vil jeg bruke personopplysningslovens (pol) krav til «behandlingsansvarlig» som eksempel, jf. pol § 2 nr 4. Denne loven innebærer for det første at det alltid skal være en som er ansvarlig for formål vedrørende behandling av personopplysninger og for tilhørende bruk av hjelpemidler. Dette er særlig krevende dersom det er flere virksomheter som samarbeider om å samle inn og bruke opplysninger om enkeltpersoner, for eksempel som ledd i felles identitetsforvaltning og andre rutiner knyttet til nettjenester, jf. for eksempel samarbeidet om Altinn. Nevnte lovs § 13 og kapittel 2 i forskriftene til loven stiller nærmere krav til hvorledes arbeidet med informasjonssikkerhet skal organiseres, og setter herunder krav til hvorledes forholdet til medkontrahenter (kalt «databehandler») kan være, jf. pol § 15.

Det er forholdsvis sjelden at en i lovgivningen stiller direkte krav til organisering. Langt oftere gjelder rettslig regulering organisatoriske spørsmål på mer indirekte måter. For eksempel legger bestemmelser om taushetsplikt og innsynsrett mv. klare føringer på hvilke samarbeidsformer som er mulige innen en viss organisasjonsstruktur. Så lenge det ikke er lovfastlagt hvorledes organiseringen skal være vil det imidlertid ofte være mulig å styre rundt slike hindringer ved å treffe avgjørelse om endret organisering. En kommunesammenslåing vil for eksempel kunne gi bedre grunnlag for informasjonsutveksling fordi det som tidligere var to forvaltningsorganer er slått sammen.

8 Juristers plass ved utvikling av beslutningssystemer

Jeg har understreket at utvikling av elektronisk forvaltning bl.a. innebærer ny organisering og nye arbeidsmåter for forvaltningens utøvelse av myndighet i enkeltsaker. Det er da nødvendig å utvikle informasjonssystemer og organisatoriske løsninger noe som krever bred kompetanse blant de personer som skal delta. Bl.a. er det behov for folk som kan ta stilling til hva det rettslige rammeverket krever, transformere jussen for å automatisere (deler av) saksbehandlingen, analysere arbeidsprosesser, fastlegge informasjonssystemenes brukergrensesnitt og design, fastsette krav til informasjonssikkerhet, ta stilling til spørsmål om teknologisk plattform og maskinvare, programmere systemspesifikasjoner, gjennomføre opplæring av ansatte mv. Uansett størrelsen på utviklingsprosjekter er dette uhyre sammensatt og krever mange ulike typer kompetanse. Et spørsmål er på denne bakgrunn i hvilken grad jurister bør ha innvirkning på slike utviklingsarbeider.

Mye tyder på at det i ytterst liten grad er jurister som foreslår eForvaltningsløsningene. I stedet er det teknologer og andre som ut i fra tilgjengelige teknologiske muligheter og «oppskrifter» foreslår hvorledes forvaltningen kan

endre sin saksbehandling ved hjelp av IKT. Dels er det tale om å kjøpe ferdig utviklede systemløsninger, dvs løsninger som ikke er laget for spesielt å ivareta behov i konkrete forvaltningsorganer. Dels er det tale om at forvaltningsorganer utvikler sine egne eForvaltningsløsninger (Internett-sider, beslutningssystemer mv). Min egen forskning fra tidlig 1990-årene viste sentrale systemutviklingsprosjekter der juristene i forvaltningsorganet var lite involverte i utviklingsarbeidet.[53] Inntrykket fra praksis i Norge anno 2007 er forholdene har bedret seg noe, samtidig som det er lang vei frem til en situasjon der jurister er med på å sette dagsorden vedrørende eForvaltningen. Jurister er med andre ord fremdeles ikke sentrale når det skal fastlegges på hvilken måte forvaltningsorganene skal arbeide med enkeltvedtak i eForvaltningen. Derfor er det etter min mening en fare for at den rettskulturen som særlig jurister er bærere av, får en svekket betydning i fremtidens forvaltning.

Per i dag har jeg ikke annet enn indikasjoner på at gjennomslaget for forvaltningsrettslig tenkning jevnt over er svakt når nye eForvaltningsløsninger skal utformes. Som tidligere understreket er de utviklingsprosesser som frembringer nye løsninger meget sammensatte, og i vrimmelen av problemstillinger er det mye som tyder på at de juridiske spørsmålene ikke blir identifisert i tilstrekkelig grad. Hovedutfordringer er derfor i) å identifisere hvilke typer av rettsspørsmål som det ofte er nødvendig å ta stilling til i eForvaltningsprosjekter; og ii) å gi nærmere retningslinjer for hvorledes disse skal behandles. Etter min mening er dette en forutsetning for at jurister kan «koples på» utviklingen av morgendagens IKT-baserte saksbehandlingsrutiner – og jurister må koples på for å ivareta et akseptabelt nivå av rettslig styring og beskyttelse.

53 Se Dag Wiese Schartum: Rettssikkerhet og systemutvikling i offentlig forvaltning, Universitetsforlaget 1993, del IV «Systemutvikling i praksis».

BIBLIOTEKVEDERLAGET*

Helge M. Sønneland

I Innledning

Det norske bibliotekvederlaget har utviklet seg gjennom en mer enn 60-årig historie, og er en vel etablert ordning for å kompensere forfattere og andre opprinnelige rettighetshavere for bruken av deres verker i norske bibliotek.

Det er en kulturpolitisk basert ordning. Staten bevilger over statsbudsjettet årlig vederlag til i alt 16 fond, som så igjen fordeler midler – hovedsakelig etter søknad – til nålevende rettighetshavere. Ordningen omfatter ikke forlag eller andre utgivere.

For 2008 var det samlede vederlaget 78,6 mill kroner. Vederlaget er basert på en bestand i norske bibliotek på ca. 43 mill. verk (utlånsenheter) utgitt i Norge (eksklusive videogram), som hvert utløste et vederlag på 181,5 øre. Vederlaget er et resultat av forhandlinger mellom rettighetshaverne og Staten ved Kultur- og kirkedepartementet, og legges fram for Stortinget til endelig godkjenning og bevilgning.

I tillegg betaler Staten et vederlag på kr 3,8 mill. (2007) til Filmvederlagsfondet for bibliotekenes bruk av filmer utgitt i Norge.

II Kort historikk

Bibliotekvederlaget ble innført ved lov i 1947, i en bestemmelse i lov om folke- og skolebibliotek. Bare Danmark har en ordning eldre enn den norske. Vederlaget var den gang en prosent-del (inntil 5 prosent) av innkjøpsbudsjettet for norske folke-og skolebibliotek. Kun skjønnlitterære forfattere og oversettere var vederlagsberettiget. Begrunnelsen var primært å kompensere for det tap som bibliotekutlånet ble antatt å føre til. Det første vederlaget var kr. 35.000,-

Bl.a. som en konsekvens av kunstner-aksjonen på 70-tallet, ble disse forutsetningene forlatt (se nedenfor). I første halvdel av 80-tallet ble det oppnådd enighet om å knytte vederlaget til bibliotekenes *bestand*, og om at bestanden både i fag- og folkebibliotek skulle telles med. Etter betydelig

* Dette en oppdatert versjon av en artikkel som ble publisert på Den Norske Forfatterforenings nettsider august 2007 (http://www.forfatterforeningen.no/v2/content/bibliotekvederlaget)

press fra organisasjonene – ikke minst fra samtlige skribentorganisasjoner – aksepterte staten at også faglitterære forfattere og oversettere skulle være berettiget til vederlag.

Utviklingen i første halvdel av 80-tallet resulterte i den nåværende lov om bibliotekvederlag av 27.mai 1987.

Lov om bibliotekvederlag er i seg selv et forhandlingsresultat. Et utkast til lovtekst ble utarbeidet parallellt med og som en del av forhandlingene om bibliotekvederlag i 1983–84.Forfatter og professor Jon Bing var skribentorganisasjonenes juridiske rådgiver. Som en del av vederlagsavtalen forpliktet departementet seg til å fremlegge lovutkastet som dermed ga vederlaget en ny lovforankring.

III Forhandlingssystemet – Regelverksavtalen

På slutten av 70-tallet ble staten og kunstnerorganisasjonene enige om en rammeavtale om organisasjonenes forhandlingsrett og om konfliktløsning, den såkalte Regelverksavtalen. Det fører for langt her å gå nærmere inn på denne avtalen og dens historie – hovedpoenget her er å nevne at de konfliktløsnings-mekanismene som følger av avtalen, hele tiden har vært lagt til grunn for forhandlingene om bibliotekvederlag, selv om Regelverksavtalen lenge har vært sagt opp. Det innebærer først og fremst at dersom det blir brudd i forhandlingene skal visse spilleregler følges. Forhandlingskonflikten overføres til Riksmeglingsmannen. Dersom det etter megling fortsatt ikke oppnås enighet, legges saken fram for Stortinget. Etter at Regelverksavtalen ble lagt til grunn, har meglingsmannen vært trukket inn ved tre anledninger, hvor det så har lykkes å nå fram til enighet. Siste gang var i 1997.

IV Lov om bibliotekvederlag

Lov nr. 23 av 29.mai 1987 er en kort lov med fem paragrafer. Paragraf 1 slår fast at opphavsmenn til verk som disponeres for utlån (inklusive referansebruk) i bibliotek, skal gis vederlag ved årlig bevilgning over statsbudsjettet. Vederlaget skal betales kollektivt til fond som etableres av rettighetshaverne.

Vederlaget er kulturpolitisk begrunnet, til fremme av norsk språk og litteratur, samt som en del av livsgrunnlaget for kunstnere.

De ulike fond som mottar støtte, fordeler midlene til enkeltpersoner etter søknad. I all hovedsak gis støtten i form av arbeids- og reisestipend. For de skjønn-litterære forfattere utbetales en del av vederlagsmidlene i forhold til antall utgivelser.

Utgivere og utøvere omfattes ikke av ordningen.

At ordningen er kulturpolitisk og kollektiv, står i motsetning til om ordningen var *opphavsrettslig* basert. Etter den norske ordningen har ingen enkelt rettighetshaver noe ***rettskrav*** på vederlag. En opphavsrettslig ordning måtte også omfattet andre grupper rettighetshavere som har fått overført rettigheter til seg ved avtale (som f.eks forlag) eller ved arv, og måtte som utgangspunkt vært individuell og omfattet også utenlandske rettighetshavere.

I lovens paragraf 2 fastsettes det at vederlaget skal kalkuleres ihht et fast beløp pr. utlånsenhet. En bok er en enhet, tilsvarende er en CD en utlånsenhet. Kun utgivelser i Norge medregnes.

Kalkulering av vederlaget skjer på basis av statistikk som utarbeides av bibliotekene. Først i 2001 ble det enighet om at statistikkgrunnlaget var godt nok til å bli lagt til grunn. Særlig var skolebibliotekstatistikken usikker. Det ble derfor gjennomført særskilte undersøkelser for å kvalitetssikre denne. Så lenge statistikkgrunnlaget ikke var tilfredsstillende, ble vederlaget fastsatt som en omforenet sum.

Vederlaget pr utlånsenhet er i 2008 181,5 øre, og har steget fra 1,65.5 i 2005. Det skal indeksreguleres med 4 pst. årlig frem til og med 2011.

Etter lovens paragraf 3 fastsettes enhetsbeløpet i forhandlinger. Hvordan rettighetshaverne skal være organisert i forhandlingssammenheng er ikke presist fastsatt i loven. Staten har imidlertid akseptert at lovens krav om en felles sammenslutning av organisasjoner er tilfredsstilt ved den etablerte ordning. Den innebærer at de 25 forhandlingsberettigede organisasjonene velger et forhandlingsutvalg med 5 medlemmer, og utnevner koordinator. Departementet godkjenner den enkelte organisasjons forhandlingsrett, og lovens forutsetning er at de enkelte organisasjoner skal representere en vesentlig del av norske opphavsmenn på området.

Lovens paragraf 4 fastsetter at vederlaget skal fordeles til fond som forvaltes av rettighetshaverne. En del organisasjoner har felles fond – derfor er antallet fond (pt 16) mindre enn antallet organisasjoner som er parter i avtalen (pt 25).

Fondene kan gi støtte til den enkelte rettighetshaver, eller til formål som kommer vedkommende gruppe til gode. Det kan ikke utbetales mer enn et beløp tilsvarende 4 G (p.t. 281 000 kroner) til noen enkeltperson.

Fondene har ikke anledning til å kreve medlemskap som forutsetning for tildeling av vederlag.

I forhandlingene står partene fritt mht til for hvor lang periode avtalen skal gjelde, utviklingen i enhetspris, og andre forhold. Opp gjennom årene har den både vært fireårig og kortere. Den nåværende avtalen er som nevnt fireårig.

Blant de omdiskuterte og uavklarte spørsmål er hvordan verk i digitalt format skal behandles (i den grad de skal omfattes av vederlagsavtalen). Spørsmålet har vært tatt opp i forhandlingene, uten at man har kommet til en avklaring.

Forhandlingene mellom organisasjonene og staten resulterer mao i avklaring av det vi kan kalle *vederlagets inntektsside*, totalvederlaget. Når det gjelder *fordelingen*, er det opp til organisasjonene å avklare hva som skal gå til det enkelte fond. Det har vært enighet om at 15 % av det samlede vederlaget skal gå til ikke-litterære verk, mens 85 % går til litterære verk. Innenfor denne delen er det – bl.a. gjennom voldgift – oppnådd enighet om fordelingen, som – grovt sett – gir 60 % til den skjønnlitterære siden, og 40 % til den faglitterære. Denne fordelingen reflekterer vederlagets kulturpolitiske grunnlag. Statistisk sett er fag- og skjønnlitteratur temmelig likt representert i bibliotekene.

Beløpet som inngår i det særskilte vederlaget for bibliotekenes bruk av film utgitt i Norge, fastsettes som en omforent sum etter forhandlinger mellom Staten ved Kultur- og kirkedepartementet på den ene siden, og Norsk Regissørforbund og Norsk filmforbund på den andre, og fordeles til norske regissører og filmarbeidere gjennom Filmvederlagsfondet.

Som følge av EØS-avtalens generelle bestemmelser, som forbyr diskriminering på grunn av statsborgerskap, er krav om norsk statsborgerskap fjernet fra alle fondsvedtekter. Derimot opprettholdes krav om utgivelse på norsk eller samisk, eller at vedkommende rettighetshaver bor og virker her i landet.

V Bibliotekvederlag – «Public Lending Right» - Status i Europa og internasjonalt

1 Forholdet til EU-lovgivningen

I 1992 vedtok EU et opphavsrettsdirektiv om utleie- og utlån av opphavsrettslig vernede verk og prestasjoner (Direktiv 92/100/EEC, nå 2006/115/EC). Det fastsetter bl.a. at opphavsmannen i utgangspunktet skal ha enerett til både utleie og utlån av sine verk. Fra utlånsretten kan det imidlertid gjøres unntak, såfremt den opprinnelige opphavsmann får et vederlag for bruken i offentlig tilgjengelige institusjoner.

Vederlagets størrelse fastsettes etter det enkelte lands kulturpolitiske forutsetninger.

Som en følge av EØS-avtalen måtte direktivets bestemmelser gjennomføres i norsk lov. Det skjedde gjennom de endringer i åndsverkloven som ble gjennomført i 1995.

Det norske bibliotekvederlag oppfyller direktivets forutsetninger for å gjøre unntak fra eneretten til utlån. I den norske åndsverkloven har man derfor opprettholdt at et verk fritt kan lånes ut når et eksemplar av verket varig er overdratt – for eksempel solgt til et bibliotek.

Denne utlånsretten omfatter i Norge både litterære verk, musikkverk og audiovisuelle verk hvor eksemplarer er solgt. (I enkelte land, som Storbritannia, er utlånsretten for musikk- og filmverk avhengig av avtale med rettighetshaverne. Oppnås ikke enighet, fastsettes vilkårene av en nemnd).

Da direktivet ble vedtatt i 1992, avga EU-kommisjonen er erklæring om at den danske bibliotekvederlagsordning var i overensstemmelse med direktivet. Også den danske ordning er kulturpolitisk. Beregning og utbetaling av vederlag er basert på utgivelser i Danmark og til støtte for dansk språk. EØS-borgere med rettigheter i utgivelser som ikke oppfyller disse kravene, er ikke berettiget til vederlag.

EU-kommisjonen endret standpunkt, bl.a. på bakgrunn av en rapport om bibliotekvederlag som forelå i september 2002 (vel fem år forsinket i forhold til direktivets krav). Kommisjonen kunne konstatere at flere medlemsland ikke hadde gjennomført direktivets krav om en vederlagsordning, og reiste sak om manglende gjennomføring mot Belgia. EF-domstolen fastslo at dersom medlemslandene gjennomfører fritt utlån fra bibliotek, skal det finnes en vederlagsordning, og at andre lands manglende gjennomføring ikke unnskylder ikke-gjennomføring. Vederlagets størrelse ble derimot ikke kommentert av domstolen.

Etter avgjørelsen fra domstolen reiste Kommisjonen sak mot flere land, bl.a. Danmark og Sverige (den finske ordning er avvikende og ble derfor ikke anfektet på dette grunnlag). Kommisjonens påstand var at de to landene foretok en indirekte diskriminering gjennom å stille krav om at de vederlagsberettigede skulle skrive på et nasjonalt språk. Kommisjonen forlangte derfor at alle EØS-borgere hvis verker var representert i danske biblioteks samlinger (om enkeltheter i ordningen, se nedenfor) skulle likebehandles.

Som en konsekvens av dette åpnet EFTA-landenes overvåkingsorgan ESA sak overfor Island og Norge, med samme påstand som EU-kommisjonen hadde gjort gjeldende overfor Danmark og Sverige. De fire landene saken var aktuell for, gjorde gjeldende samme argumentasjon, nemlig at ordningene ikke er i strid verken med generelle EU/EØS-regler, eller med direktivet.

EU-kommisjonen vedtok i desember 2007 å henlegge sakene mot Danmark og Sverige. I en avgjørelse av 10. april 2008 gjorde ESA vedtak om å lukke saken mot Norge og Island.

ESA gjorde samtidig vedtak om å lukke en sak som var reist i klage av 1997, med påstand om diskriminering. Klagen gjaldt også spørsmålet om vederlag for bruk av bibliotekenes bruk av videogrammer, hvor klageren hevdet at også

produsenter hadde krav på vederlag. Dette kravet var også bestridt av Kultur- og kirkedepartementet, som hadde ment at dette ikke fulgte av direktivet.

2 Situasjonen i andre nordiske land

Som det allerede har fremgått, har alle de nordiske land bibliotekvederlagsordninger. De er imidlertid ulike. Her tar jeg bare med noen hovedtrekk:

Den danske ordningen har det største vederlagsbeløp av alle tilsvarende ordninger i verden – ca. 140 mill. DKR. Den er kulturpolitisk basert, og beregnes etter bestand av bøker i danske skole- og folkebibliotek. Danske nålevende forfattere utbetales individuelt, etter et sofistikert poengsystem som bl.a. vekter etter genre, og i forhold til sidetallet i de bøker av vedkommende forfatter som finnes i bibliotekene. Det er satt tak på maksimal utbetaling. Andre rettighetshavergrupper, som oversettere og komponister, får også vederlag, men da i form av mulighet for stipend. Vederlaget administreres av en egen enhet i Bibliotekstyrelsen (film kan i Danmark bare lånes ut etter særskilt avtale, og vederlaget for dette utbetales særskilt på bakgrunn av en opphavsrettslig basert avtale).

I Sverige beregnes vederlaget (samlet SEK 119,5 mill i 2006) etter antall utlån pr. verk i svenske folkebibliotek. Enhetsprisen er gjenstand for drøftinger. Av det samlede vederlag utbetales 60 % individuelt til den enkelte forfatter på grunnlag av utlånet av hans/hennes verk. 40 % deles ut som stipend/støtte og garanti-inntekt av Sveriges Författarfond. I Sverige omfattes også utøvere på fonogrammer av ordningen.

Også det islandske vederlag beregnes etter utlån, og tildeles individuelt. Både det svenske og islandske vederlag er kulturpolitisk basert. Det gjelder også det finske vederlag, som imidlertid er en statlig bevilgning som ikke er relatert til verken bestand eller utlån.

Også på Færøyane og Grønland er det bibliotekvederlagsordninger, begge basert på bestand.

Som i Norge, omfatter vederlagsretten heller ikke i de øvrige nordiske land forlag eller andre produsenter.

3 Situasjonen i EU

Selv om kravet om å etablere en vederlagsordning som nevnt følger av et direktiv som nå er mer enn 16 år gammelt, har innføringen av bibliotekvederlagsordninger gått tregt både blant tidligere og nye medlemsland. Etter at saken mot Belgia hadde avklart at leie-/lånedirektivet medførte en rettslig

forpliktelse til å etablere i det minste et visst mimum av vederlagsordninger, har EU-kommisjonen det siste tiår klaget flere land inn for EF-domstolen.

Ut over de nordiske land, og EØS-medlemslandet Liecthenstein, har EU-medlemmene Storbritannia, Tyskland, Nederland, Luxemburg, Østerrike, Estland, Latvia, Litauen, Kroatia og Slovenia etablerte ordninger, de fleste basert på utlån.

Frankrike innførte sin ordning med virkning fra 2007. Denne som flere andre av ordningene gjør også forlag vederlagsberettiget.

Belgia, Portugal og Spania er av EF-domstolen pålagt å etablere ordninger, og disse er vedtatt og under etablering. Tsjekkia startet utbetalinger fra sin ordning i år. Øvrige EU-land som ennå er uten ordning, eller som ikke er godt på vei til å gjennomføre planleggingen, har mottatt klage fra EU-kommisjonen, som må forventes å ta saken inn for EU-domstolen for ikke-oppfyllelse av direktivet.

Pr. september 2007 – da den siste internasjonale konferansen om bibliotekvederlag ble arrangert i Paris, var følgende land registert uten ordninger: Irland, Polen, Romania, Slovakia, Ungarn, Bulgaria, Malta, Kypros og Hellas.

Det generelle bildet er at staten utreder vederlaget gjennom en bevilgning over statsbudsjettet, men dette er ikke uten unntak:

I den nederlandske ordningen, som er den eneste som er helt ut opphavsrettslig, betaler nederlandske folkebibliotek av eget budsjett, og de krever en mindre medlemsavgift av sine brukere.

I visse tilfelle tillates ikke bøker utlånt før etter en viss karenstid etter utgivelse. I Spania er forutsetningen at bibliotekinstitusjonene eller deres eiere betaler vederlaget.

Den tyske ordningen er delvis kollektiv idet ca. 30 prosent av vederlaget går til sosiale formål til beste for rettighetshavere. Den øvrige del er individuell og i prinsippet opphavsrettslig basert.

I Storbritannia utbetales på kulturpolitisk grunnlag individuelt til forfattere på grunnlag av utlån i folkebibliotek. Det samlede vederlagsbeløp fastsettes av departementet i form av en årlig bevilgning.

Utlån av musikk og audiovisuelle verk må etter britisk lov baseres på avtale, og vederlag utbetales individuelt gjennom rettighetshavernes forvaltningsorganisasjoner. Oppnås ikke avtale, fastsettes som nevnt vilkårene av en nemnd.

Her skal det skytes inn: Spørsmålet om en ordning er opphavsrettslig eller ikke, må avgjøres etter en konkret vurdering av hvordan ordningen er bygget opp og virker. Hva de enkelte land selv erklærer sin ordning for å være, er ikke avgjørende, heller ikke om den er etablert ved egen lov og ikke i vedkommende lands ånsdsverklov: Dersom ordningene de facto gir den enkelte rettighetshaver som er representert i et bibliotek et rettskrav

på vederlag i forhold til bruk – enten det gjelder bestand eller utlån – vil ordningen avhengig av situasjonen kunne bli ansett som opphavsrettslig. Det innebærer i så fall at i alle fall alle EØS-borgere må gis like retter, samt at også arvinger og utgivere må tilgodeses. I Europa må det legges til grunn at EF-og EFTA-domstolene har kompetanse (bl.a. gjennom leie-/ lånedirektivet) til å treffe avgjørelser om hvordan det enkelte vederlag er å anse.

Norsk faglitterær forfatter- og oversetterforening har det siste tiåret spilt en aktiv rolle i arbeidet med å etablere bibliotekvederlagsordninger i europeiske land, og tok i sin tid initiativ til det som er blitt et forum for bibliotekvederlag med fokus på Europa. European Writers Congress spiller her en viktig rolle. Gjennom konferanser i de aktuelle europeiske land har man ønsket å stimulere forfatterorganisasjoner og myndigheter til å etablere bibliotekvederlagsordninger til beste for forfattere og andre opprinnelige rettighetshavere.

4 Situasjonen internasjonalt

I tillegg til i de europeiske land som er nevnt, finner vi bibliotekvederlagsordninger i Australia (fra 1974), Canada (fra 1986), Israel (fra 1986) og New Zealand (fra 1973). Av disse fire er den israelske basert på utlån, de øvrige på bestand, og alle er kulturpolitisk fundert. De har – som i Europa – ulike avgrensinger, og gjelder i hovedsak folkebibliotekutlån.

Det britiske forvaltningsorganet – Public Lending Right – tok i 1995 initiativ til en konferanse for land som har innført eller planlegger å innføre bibliotekvederlag, internasjonalt betegnet som PLR. Det har til nå vært gjennomført syv konferanser. De norske organsasjonene i samarbeid med Kultur- og kirkedepartementet arrangerte en slik konferanse i Oslo 2003. Disse konferansene er først og fremst ment å gi grunnlag for idé – og erfaringsutveksling, men også mer generelle tema har vært drøftet. Forholdet til opphavsretten er blant disse. Det samme gjelder behandlingen av materiale i digital form (ingen land har ennå avklart dette spørsmålet), og avgrensningen av grunnlaget for beregning av vederlag. Norge er det eneste land hvor vederlaget gjelder for alle bibliotekvirksomheter, dvs at også samlingene i fag- og forskningsbibliotek og Nasjonalbiblioteket inngår i beregningsgrunnlaget.

Storbritannia og Tyskland og Nederland har åpnet for utveksling av vederlagsmidler under forutsetning av gjensidighet. For Nederland og Tysklands del kan en merke seg at gjensidighetskravet er gjort gjeldende selv om det i disse landene er tale om helt eller delvis rent opphavsrettslige ordninger, og hvor Bernkonvensjonens generelle krav er at vederlagsretten normalt skulle gjelde

verk fra alle unionsland. Her kan en også notere at en slik praksis ser ut til å være akseptert de facto i internasjonale organisasjoner, og under forhandlinger om nye instrumenter gjennom de siste 25 år.

Storbritannia og Tyskland har inngått en slik gjensidighetsavtale om utbetalinger av vederlag. Den omfatter knapt NOK 100 000. Det tyder på at tilgjengelige data er utilstrekkelige for gjennomføring av individuelle utbetalinger på tvers av grenser, selv om dette skulle bli et pålegg.

VI Noen betraktninger om fremtiden

Som det fremgår ovenfor, har EU-kommisjonen og ESA satt spørsmålstegn ved om den norske (og de islandske, svenske og danske) ordningene oppfyller EU/EØS-rettens krav. Det ble ikke bestridt at ordningen kan være av kulturpolitisk karakter, men det ble krevd at vi forlater kravet om norsk eller samisk språk som grunnlag for vederlag, fordi dette indirekte er diskriminerende.

De danske myndighetene påtok seg under sakens gang å være de nordiske ordningenes fremste fanebærer overfor påstandene om at leie-/lånedirektivet ikke er riktig gjennomført; allerede i 1992 var Danmark, som eneste nordiske EU-medlemsland, klar over at ordningene måtte beskyttes. Danske, svenske og norske myndigheter hevdet med styrke at de ikke kunne se at noe har skjedd siden 1992 som skulle gjøre at konklusjonene fra den gang må endres.

Både EU-kommisjonen og ESA har – om ikke for alltid – lukket sakene. Men for den – forhåpentligvis lite sannsynlige – eventualitet at de igjen skulle åpnes og situasjonen endres, er de norske rettighetshaverorganisasjonene og staten enige om at kortene må legges på nytt. En konsekvens av lojalt å gjennomføre EU-kommisjonens opprinnelige krav vil nemlig være at en stor del av de norske midlene må sendes til utlandet – et resultat av det faktum at vi er et kulturimporterende land. (En skal være mer enn alminnelig optimistisk anlagt for å tro at det norske vederlaget blir hevet, slik at norske rettighetshavere etter en endring beholder samme beløp som i dag).

Dersom de sakene EU åpnet mot Danmark og Sverige, og ESA mot Norge og Island, ikke var blitt lukket, er det rimelig å anta at dette kunne fått negative konsekvenser for både tempoet i etableringen og omfanget av bibliotekvederlagsordninger i de medlemsland som ennå ikke har oppfylt sine forpliktelser etter leie-/lånedirektivet.

VII Avsluttende bemerkninger

Bibliotekvederlaget er – slik det gjentatte ganger har vært fremhevet i ulike stortingsdokumenter – et viktig virkemiddel i norsk kulturpolitikk, være seg

språk-, litteratur- eller kunstnerpolitikk. Det har det i alle år vært bred politisk enighet om. Den norske ordningen har utviklet seg gjennom mange år. Den er vel forankret, og er relativt enkel å forvalte – i alle fall om man sammenlikner med de administrative systemer som kreves for å gjennomføre ordningene i de fleste andre land.

Det norske vederlag har – som i andre nordiske land – et betydelig omfang om en sammenlikner med ordningene som ellers finnes, både i absolutte beløp, og særlig i forhold til folketall. Ikke uten grunn er det derfor den norske og de øvrige nordiske ordningene blitt fremhevet i de internasjonale fora hvor denne type vederlag blir diskutert.

Det er å håpe at de spesielle internasjonale konferansene vil bli fulgt opp. Irland – som ennå ikke har etablert noen vederlagsordning – har påtatt seg vertskapet for neste konferanse i 2009. Det er neppe spesielt radikalt å spå at det i kommende år vil skje betydelige endringer i så vel bokbransjen som i bibliotekverden, bl.a. som følge av digital teknologi. Hvordan utviklingen kan tenkes å påvirke bibliotekvederlaget vil bli et interessant tema i de kommende diskusjoner.

TAKING ADVANTAGE OF NEW TECHNOLOGIES: FOR AND AGAINST CRIME*

Maryke Silalahi Nuth

Abstract

Advancement in the field of Information Communication Technologies (ICTs) changes not only our society but also crime. It opens more opportunities for crime and draws people into committing crime, leading to an unprecedented growth in the crime rate. On the other hand, it has also been applied to criminal justice. Crime fighters use the ICTs to control crime and gain efficiency in their policing efforts to service the community. This has led to more effective police work. As both criminals and police benefit from ICTs, these new technologies create new pitfalls for both criminals and law enforcement. Use of technologies by criminals represents challenges and risks to the crime fighter and *vice versa*. This triggers a crime race and raises notable social concerns on the adverse use and potential abuse of ICTs. Proactive territorial-based regulations, although called for, do not always provide solutions. The borderless nature of ICTs may not allow for rigid regulations and instead challenges the principle of criminal laws. As such, international laws and regulations combined with reliance on technologies are crucial to counter the crime race.

Introduction

Crime is a major social and legal problem in the world we live in. It triggers fear but at the same time evokes profound fascination. It challenges the normative order and simultaneously marks the limits of the law. Confronting crime means facing the reality of constant change in our society. Crime changes with time and circumstances. As society develops, crime develops. Often, things that facilitate social development also do the same to crime. New technologies, which undoubtedly have a significant role in the changes in our society, are constantly being exploited by both criminals and crime fighters. Criminals use new technologies to facilitate and maximise criminal activities,

* This article was previously published in Computer Law and Security Report, vol. 24 (5) 2008, pp. 437–446.

while police use new technologies to do the opposite, i.e. minimizing or controlling criminal activities.

This article will look into how criminals and crime fighters take advantage of new technologies, with considerable emphasis on ICTs. This paper is not an attempt to provide an exhaustive list or extensive descriptions of new technologies to assist or combat crime. Rather, the technology is briefly discussed to elaborate how its exploitation affects not only those who exploit it but also the face of crime and society in general. Indeed, the application of new technologies has brought many advantages to the police's work and society in general. Nevertheless, criminals also enjoy benefits from using ICTs in their practices. Therefore, the concern on appropriate, responsible and legitimate use of ICTs becomes more significant than ever.

1 Application of New Technologies

1.1 Crime Enhancing Technology

New technologies bring new opportunities for criminality. With the help of globalisation, such opportunities are rising at an «unprecedented rate».[1] New technologies have now become the subject (place), object (target), tools (instrument) and symbol of crime.[2] This is especially true in case of the Internet, a network of computer networks. When first introduced, the Internet was no more than a communication tool to exchange messages. As Internet technology advances, it is now possible to connect practically any computer in the world to the Internet. Connecting to the Internet means connecting to millions of computers or computer networks located in different part of the world and interconnecting with each other. Territorial space is no longer a hurdle; the Internet is globally available and can be accessed easily from anywhere at any time and at a reasonably low cost (if any). Although some parts of the world have minimal or no access to global communication networks at this moment, there is no reason to suggest that this will be permanent. All countries want to connect globally and efforts to reduce the digital divide are constantly being pursued. The Internet is an essential infrastructure for such global connection.

1 Gloria Laylock, «New Challenges for Law Enforcement», European Journal on Criminal Policy and Research 10: 39–53, 2004 at p. 39.

2 Ernesto U. Savona & Mara Mignone, «The Fox and The Hunters: How IC Technologies Change the Crime Race», European Journal on Criminal Policy and Research 10: 3–26, 2004, at pp. 7–11.

For criminals, the Internet is like a gateway to an enormous level playing field. Internet makes it possible for criminals to *access* the information communication systems, and thus lives, of great numbers of people in various jurisdictions. Thus, the potential and impact of crime committed on, or facilitated by, the Internet are enormous. What's more, a criminal does not even have to be physically present in a particular jurisdiction to pursue crime. He or she can be in a remote location in the Pacific while at the same crashing the European stock markets.

Various terms have been used to give a name to crime conducted in the Internet, such as cyber crime, Internet crime, computer crime, computer-related crime, etc. Whatever word is used, these terminologies imply that the advent of technology has a significant role in: (i) making criminal offences possible, (ii) creating (new) criminal offences and/or (iii) transforming traditional crime into modern crime. The computer, which made the Internet possible in the first place, is used as the primary tool to facilitate crime and the target thereof, hence the term «computer crime». This includes a broad range of crime targets, including those made possible by using a computer system, computer data, or computer products and services.[3] Technology can transform old crime into new modern forms. With the help of computers (and the Internet), traditional crime is committed in new ways and is thus called «computer related crime» or «computer facilitated crime».[4]

There is nothing new with regards to using technology as an instrument of crime or as object of crime. People have long used technologies in designing or committing their crimes. What is different now is the extent to which criminal activities can be committed. New technologies make it easier to commit existing crimes. Counterfeit documents, threats, child pornography images, hate speech and defamatory information can all be generated and spread by a computer in a matter of seconds to millions of computers around the world. Offences against property, which traditionally have been executed by other means, can now be executed via the Internet, a computer related venue or some other technological computing advancement. These include infringements of intellectual property rights, fraud (business, investment or computer and Internet fraud), economic espionage, theft and embezzlement.[5] At the

3 Offences could be in the form of unauthorized use or access to a computer system; the unauthorised copying, altering, deleting, or destroying of computer data, software or programs; disrupting computer services or denying computer services to an authorized user; spreading malicious computer viruses into computers or computer systems; and misuse of someone else's Internet domain name.

4 Savona & Mignone, supra note 2, p. 10.

5 Savona & Mignone, supra note 2, p. 11.

same time, entirely new types of crime such as cyber stalking, cyber bullying and cyber-money laundering are also emerging. Cyber stalking, which is repeated harassment and threatening actions online, consists of following people and watching their online movements overtime, for the purposes of intimidation, sexual domination or other motives.[6] Children and teenagers cyber bully by picking on a victim through web postings or mass emails, and spreading harassing online messages containing sensitive personal information or threatening to harm the victims.[7] Cyber-money laundering is the online act of making money looks like it was obtained from legal sources when, in fact, it was obtained through illegal activities. It could be described as fencing currency, and thus also is known as e-fencing.[8]

The list of crime technology and crime innovation is long and ever growing. Still, lots of other crime can be added to the list, such as spreading computer viruses, cyber-vandalism and hacktivism. Computer viruses can be very destructive, and some of them can even act as spyware. The viruses search for passwords, credit card numbers, contact details or other information and then forward this information to the authors of viruses. Alternatively, such information can simply be spread online so that anybody can access or pick it up and, as a result, the data owner is placed in a vulnerable position. These viruses can be disguised as heading-friendly emails or unsolicited commercial email communication (spam) with attachments. Once the attachment is opened, viruses are released and multiply themselves rapidly to attack the computer system. In 2000, the computer virus «love bug» managed to affect millions of computers around the world within a few hours and exposed many corporate and government information systems to virus attack. The first five days alone of the spread of this virus was estimated to cost worldwide businesses $6.7 billion.[9]

Cyber-vandalism (malicious destruction or defacement of property), which is often conducted by teenagers, at its most extreme, can interrupt the computer systems of organisations across the world. Hacktivism, network attacks targeting human/computer interface on the Internet by use of hacking techniques, is mostly committed with the purpose of disrupting service without

6 Samuel C. McQuade III, Understanding and Managing Cybercrime, Pearson Education, Inc., 2006, pp. 95–96.

7 McQuade, supra note 6, p. 94.

8 This new type of crime is usually conducted on online auction sites such as eBay where thieves and fraudsters sell stolen goods and counterfeit merchandise, often at a large discount off their face value. See further: «e-fencing: Hawking Stolen Goods on eBay», Loss Prevention News, 13 October 2007, available on http://www.hotlpjobs.com/, last accessed 17 April 2008.

9 Graeme R. Newman & Ronald V. Clarke, Superhighway Robbery: Preventing E-Commerce Crime, Willan Publishing, 2003, p. 53.

necessarily causing serious damage. Previously, hacktivism was defined as physical or syntactic network attacks but nowadays it has come to refer to semantic attacks because it targets «the way we, as humans, assign meaning to content» and such semantic attacks are believed to be more serious than physical or syntactic attacks because it is targeted at «the human/computer interface, the most insecure interface on the Internet.»[10] Most common attacks include virtual blockades and automated email bombs. Politically motivated hacking techniques used systematically in an effort to cause grave harm, such as loss of life or serious economic damage, are popularly known as cyber terrorism.[11] An example is hacking into a traffic control system for the purpose of creating transportation chaos and causing death in traffic collisions in an effort to overthrow a government. Cyber terrorism also is often used to try to eliminate a particular group of race, ethnicity or religion.[12]

Stealing, one of the most common motives for Internet financial crimes, can be accomplished in various ways with the help of technology. Identity theft occurs when someone's personal information is used by a criminal to take on that person's identity, such as opening a new credit card, taking up a loan or shopping online in that person's name. Identity theft is often made possible by *phishing*, or tricking consumers into disclosing their personal and financial data such as password information, credit card or bank account details. The most common modus operandi is spreading official-looking emails from large internet banking and online services requiring customers to 'confirm' some personal and financial details. Internet *pharming* is another method used for phishing in which Internet traffic is illicitly redirected to targeted websites; once there, users are tricked into giving away sensitive information. Recently, hackers have also extended phishing practice to net phone systems. Scams which were previously email-based can now avoid the email system altogether. Computers are programmed to dial a long list of phone numbers and play a recorded message to anyone that answers. The message more or less contains warning about the fraudulent use of a credit card and instructions to enter the card number and security number found on the rear of the card for verification.

10 Bruce Schneier, Semantic Attacks, The Third Wave of Network Attacks, Crypto-gram Newsletter, 2000, available on: http://www.schneier.com/crypto-gram-0010.html, last accessed 23 April 2008.

11 Dorothy E. Denning, Activism, Hacktivism and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy, available on http://www.iwar.org.uk/cyberterror/resources/denning.htm, last accessed 23 April 2008.

12 McQuade, supra note 6, pp. 102–103.

1.2 Crime Fighting Technology

It should be noted that the term «ICTs» encompasses many aspects of information technology. It is not limited to the Internet, but covers any technology that helps to produce, store, transmit, communicate and/or disseminate information in all forms, including in forms of voice, text, data, graphics and video. These technologies have long been applied to criminal justice. Efforts to tackle the challenges of crime have always been assisted significantly by developments in technologies. Crime detection and prevention technologies are constantly being developed to help police in carrying out their work, and have become a fact of life in modern society.[13]

The advance of surveillance technologies has helped in deterring crime and facilitating the identification of offenders. Despite the concern of crime displacement, installing surveillance technologies in public spaces may help in reducing crime. An example is the installation of the Closed Circuit Television (CCTV) surveillance system in confined public spaces and commercial establishments in the United Kingdom (UK). CCTV was introduced with the intention to reduce crime and, to some extent, has been successful in doing so.[14] In 1990 there were only approximately 100 cameras within CCTV's three schemes. By 2002, the number of cameras is estimated to have reached a staggering 500,000 in London alone.[15] Some research papers have found that within the wide areas covered by CCTV there is a significant crime drop when compared either to a period prior to the installation or to control areas without CCTV.[16] It has also been noted that CCTV did not only help police in detecting and arresting offenders, but has also helped to identify missing or lost persons. Since UK courts consider records of images captured by CCTV as convincing evidence, the system saves litigation time and costs because it increases the likelihood of a guilty plea.

---

13 See generally: Michael Bromby, «Security against Crime: Technologies for Detecting and Preventing Crime», International Review of Law Computers & Technology 20: 1–5, 2006.

14 Some studies have shown that, depending on the context and method of implementation, CCTV sometimes works and sometimes does not work as expected. See: Rachel Armitage, «To CCTV or not to CCTV: A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime», Nacro Community Safety Practice Briefing, 2002, available on http://www.epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf, last accessed 14 April 2008.

15 Michael Mc Cahill & Clive Norris, «CCTV in London, Center for Criminology and Criminal Justice», Working Paper No. 6, University of Hull (United Kingdom), 2002, p. 20.

16 Detailed studies and evaluation of CCTV include: Nick Tilley, «Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities», Working Paper No. 42, Crime Prevention Unit Series, HSMO, 1993; Kate Painter & Nick Tilley, Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention, Criminal Justice Press, 1999.

The Global Positioning System (GPS), a satellite-based navigation system for tracking location, has now been extended to mobile phones and automobiles. With GPS, it is now possible to identify a particular location with precision and minimal time. This may be crucial not only in locating suspects or fugitives, but also in saving lives (of the victims) and providing help for officers in action. GPS in private cars is beneficial not only for the car owners, but also for police work in case of theft. An example of this is the LoJack car security system. This system involves several small concealed transmitters hidden in a vehicle (sometimes in the chassis of the vehicle), which are connected to satellite.[17] This option is very useful in case of theft, accidents or simply car breakdowns, because it can facilitate intelligent assistance or recovery of the vehicle. Time can be saved and police or rescue work will be more effective.

Police have also endorsed and recommend the use of personal safety alarms embedded with GPS technology. Investigations have shown that victims are usually too traumatized to shout for help in unfamiliar and dangerous situations, especially when they are isolated and vulnerable. Portable personal alarm systems enable victims to make contact with others when in need of assistance by simply activating the alarm. Some personal alarm systems, such as the violence alarm, are linked to an alarm central or police quarters. This enables police to locate the victim and react immediately when the alarm is activated. Similarly, personal (alarm) location systems are used by police to monitor the movement of persons on bail or probation, or under restraining orders. This electronic tagging, although it restricts liberty, allows police to obtain knowledge of whether curfew orders are respected. It has been suggested that this kind of system is better than CCTV because, while CCTV presents the risk of crime displacement, this electronic tagging «appears to reduce re-offending» or prevent crime.[18]

Police efforts in detecting crime have also been helped by a variety of technologies. The development of DNA testing in forensic science has permitted the identification of victims and links subjects to crime scenes with a precision not previously considered possible. In the US, this technology has also been used to exonerate wrongly convicted persons and, by doing so, preserve justice.

Police work in detecting crime or potential offences has also been made more efficient by ICTs. Much police technology is either computer-based or at least involves computers in its functioning. New technologies make manual search unnecessary, and police do not need to conduct invasive searches on a

17 More information on the LoJack car security system is available on: http://www.lojack.com/.

18 Bromby, supra note 13, p. 3.

person's body or particular object. To detect concealed weapons, police can use new technologies such as Infrared Imaging, Millimeter Wave Imaging and Acoustic Imaging.[19] Infrared spectroscopy can substitute trained police dogs in identifying illicit drugs. Similarly, Magnetic Resonance Imaging (MRI) can detect illicit substances inside the human body. Modern giant scanning machines placed at borders or ports detects not only smuggling, but also bombs or nuclear radiation, as in the case of the Hong Kong border security system.[20] Containers entering or leaving Hong Kong ports must pass through two giant scanners. One checks for nuclear radiation, while the other checks for any suspicious object made of steel or lead that could shield a bomb from the nuclear detector. X-ray-like images of the passing containers and the tracking code of each container are recorded in the computer server. This information can be used to identify suspicious cargo before it gets loaded onto a ship, or to track the cargo at any point along its journey. This has been perceived as a vital security strategy for uncovering smuggling activities, as well as for the war on terrorism worldwide.[21]

Technology can also make criminal activities difficult to conduct or, in some cases, almost impossible to commit. Access control based on retinal imaging, voiceprints, palm hand geometry or other biometric identification blocks access to those not listed in the computer database. Digital rights management systems embedded in copyrighted works permits only the legal performance of rights. Smarter lock technology embedded in televisions, electronic players or car radios prevents the device from functioning if it is removed from where it is installed. The list can go on and is ever growing.

---

19 Long Wave Infrared Imaging detects a weapon by showing its cooler image against the body's heat emissions. Similarly, Millimeter Wave Imaging also measures energy radiated from human body to detect weapons. Although it provides poorer imaging quality than Long Wave Infrared Imaging, it can penetrate clothing, which other technologies can not usually do. Acoustic Imaging focuses on the energy of the weapon. See: US National Institute of Justice, Technology for Policing, Conference Report, 1996.

20 The Hong Kong border security project was launched as a 100% cargo container scanning process and was claimed to be successful in electronically scanning each and every container entering and leaving Hong Kong port during its operation. Hoping that the same technology would be adopted in the US, the Hong Kong port authority requested funding from the US in 2005 to continue the project, but did not receive any. The 100% scanning project was eventually shut down in November 2006; container scanning still continues, but not for all containers.

21 Alex Ortolani & Robert Block, «Hong Kong Port Project Hardens Container Security», The Wall Street Journal, 29 July 2005.

1.3 ICTs and Policing Efforts

Policing has an increasing dependence on ICTs. Progress in modern policing and corrections has often been measured in terms of technical innovations.[22] The success of anti crime agendas built on community-based crime fighting is often made possible by technologies. Community policing,[23] which has been around for decades, also embraces technology in its implementation. In fact, the beginning of the community policing era in 1970 was marked by the widespread introduction of computers to policing. Communication technology has opened policing to the community. It facilitates information sharing and can mobilize the community around salient crime and quality of life issues. Information dissemination helps the community to better understand policing, and helps police to better understand community issues and restraints. Proper technology in the right management system enhances police ability to analyse and address community problems in a systematic manner.

The impact of ICTs on police organizations has also been examined by Hughes and Love.[24] They argue that although some benefits can be gained from the evolution of earlier police organizational practices, i.e. from ethnocentric, polycentric to geocentric profiles (from local operational dependence to a worldwide interdependence orientation),[25] it is now time to include «cybercentrism» in the police management style. They characterised cybercentrism as «… management of highly interactively digital economic universe, capturing a 'real time' vision of market realities without physical size limitation to corporate operations or growth».

The cybercentrism concept evolves around the idea that in order to satisfy customer expectations, managers must adopt a new approach to do business. Hughes and Love noted that in geocentric style management, where the focus is «worldwide interdependence», the cost of providing world orientation

22 Peter Grabosky, «Technology and Crime Control», Trends and Issues in Crime and Criminal Justice No. 78, Australian Institute of Criminology, 1998, p. 1.

23 Community policing is a policing strategy and philosophy that strives to make police part of the neighbourhood by encouraging police interaction with community members. It is believed that support and help from community members are significant in the success of the police's work in crime control as well as in solving other community problems.

24 Vincent Hughes & Peter E.D. Love, «Toward Cyber-centric Management of Policing: Back to the Future with Information and Communication Technology», Industrial Management and Data Systems, Vol. 104, Nr. 7: 604–612, 2004.

25 Earlier organizational profiles were developed in the late 1960s and classified based on orientation. Ethnocentrism focuses on «home country orientation with overseas operation as secondary», polycentrism has «host country orientation with subsidiaries established in overseas market» and geocentrism has a worldwide orientation. For further discussion on these profiles, see: Hughes & Love, supra note 20, pp. 606–607.

is very high mainly because of spatial, communication and cultural barriers. There are high costs for travel and education, and a large amount of time spent in making decisions due to geographical locations. The inclusion of a cybercentric style of management can transcend organisation «from a 'place' or the terrestrially grounded orientation to a 'space' or virtually extended organisation». They further argue that police managers nowadays are compelled to become familiar with virtual organization because ICTs are crucial for the success of any modern policing.

1.4 CompStat

An example of the critical and successful use of ICTs in modern policing can be seen in the implementation of CompStat in the United States (US), a concept often considered to be one of the most important organizational/administrative innovations in policing during the latter half of the 20th century.[26] CompStat (short for COMPuter STATistics or COMParative STATistics) is the accountability process and organizational management tools for police departments in the US. It was first implemented by the New York City Police Department in 1994 and since its implementation; crime fell sharply throughout the city of New York.[27] Although there have been continuing debates on the true reason for the crime drop, many experts argued that CompStat did play significant role.[28]

Central in the CompStat concept is the use of hard data combined with the stepped-up accountability of police managers. Each week, borough and precinct commanders must present a plan in the CompStat meeting to make progress on the city's crime strategies. To make their plans credible, they must be based on a current picture of crime and quality of life in their respective communities. Therefore, those commanders must have accurate and timely mapping support. To implement the system, data were collected and transformed into elementary databases using simple software programs. The locations of the seven major

26 Due to its success, CompStat has been copied and implemented not only by police in other regions in the US, but also by other government organisations. Trafficstat, Healthstat, Parkstat, Homestat and Jobstat are examples of CompStat-inspired management systems. See: Rebecca Webber & Gail Robinson, «Compstatmania», Gotham Gazette, 7 July 2003, available on http://www.gothamgazette.com/article/issueoftheweek/20030707/200/432, last accessed on 18 April 2008.

27 Overall the crime rate in 1994 was 65 percent lower than that of 1993.

28 Some commentators have claimed that CompStat's role in the crime drop has been minor, and argued that the prevailing social, economic and demographic conditions when CompStat was introduced were core contributors to the drop. See: Eli B. Silverman, NYPD Battles Crime: Innovative Strategies in Policing, Northeastern University Press, 1999, pp. 4–19.

crimes that municipalities must report to the US Federal Bureau Investigation were mapped and displayed by putting pins on conventional maps on the wall. Since this humble start, a lot has changed. To look at patterns of crime in a particular precinct, a user now needs only to click on the precinct desired and the computer will display types of crime committed, period of time analyzed, etc. To keep the information in the system current, complaint reports are now being entered directly into the database instead of being typed on traditional carbon-copy paper and manually distributed. The computer will then generate (electronic) maps of crime locations citywide, as well as graphics of notable changes and emerging problem spots. The map shows not only a street grid but also the locations of important geographical sites such as bars, restaurants, subway stations, schools, and parks.

During CompStat weekly meetings, the statistics, maps and graphics will be displayed and used as the basis to (i) analyze geographical locations of crime and correlations between crimes and why they are occurring, (ii) monitor crime patterns and (iii) discuss crime strategies, including ideas for the development of advanced computerized crime tracking methods. Information generated and made visual by computers assists police managers in analysing potential crime and identifying emerging trends early enough to implement necessary changes in the current or proposed measures without wasting resources, time and money. In turn, this will enable police managers to generate the implementation of effective crime strategies, including the appropriate deployment of resources to fight crime as well as appropriate measures to meet the community and political expectations.

The Internet also has a significant role in CompStat's implementation. Crime statistics from boroughs and precincts are published on a regular basis on the Internet. People can track weekly statistics of the CompStat data that are provided with a historical perspective of the crime drop from 1990 until 2007.[29] It is also possible to access the profiles of commanding officers and, as such, society is provided with visible accountable faces. For people of New York, this can arguably provide (re)assurance that police officers with credibility (as can be extracted from police profiles) are doing their jobs as well as guarding the community. The greater concern of a concurrent decline in confidence in the police can also be addressed, because the police's success story in the crime drop can be used as a means to gain legitimacy for policing decisions. As such, the Internet helps not only to implement community policing, but also to facilitate reassurance policing. Like in any other policing

29 CompStat data can be accessed via the website of New York City Police Department: http://www.nyc.gov/html/nypd/home.html.

environment, ICTs provide police managers with tools to meet strategic challenges by facilitating and aiding problem solving, improving service delivery and enabling efficiency.

2 Identifying the Challenges

2.1 Two Sides of the Same Coin

In light of the above, it appears that the list of technologies used for and against crime is rather long. The list is far from exhaustive, but it shows that technologies have changed the way in which both criminals and police work. It shows that both criminals and police gain considerable benefits from exploiting new technologies. These benefits are in fact both a risk and a challenge to their respective counterparts. Exploitation of technologies by criminals is an inherent risk for law enforcement and *vice versa*. The role of technology in providing more opportunities for criminality is a challenge for police work and, at the same time, police utilization of technology in controlling crime is a challenge for criminals.

2.1.1 Change of Practices

New technologies have changed the way both criminals and police conduct their activities. Surveillance technology allows actions to be coordinated at a distance. Police can guard community safety and security without the demand of direct physical appearance. Criminals use this technology to watch their targets, design crimes and avoid detection during the commission of a crime. Other technology, such as the Internet, enables criminals to remotely control attacks on computers or computer networks, such as in sending phishing e-mails, hosting spoofed websites for pharming scams and distributing malicious viruses. Corporate or intellectual property espionage can be conducted by planting Trojan horse software in competitors' computers to access confidential information or facilitate online extortion. There is no need for a spy's physical appearance because technology acts as spy for him or her.

Nowadays, the police no longer need to conduct often painstakingly long manual searches on wide territorial areas in cases of missing persons, theft or fugitives. Technology of location can assist police in determining the location of subjects or objects almost immediately and with precision. Criminals also use this technology to locate targets and ensure their criminal activities run smoothly. Manual criminal practices are being replaced by advanced technology. Traditionally credit card skimming was done by retail workers who

manually swiped a credit card through a handheld scanner before swiping it through the business card scanner. Nowadays, a micro chip installed in the business card scanner can copy the information from the credit card's magnetic strip. Once the scanner is connected to a phone line, such data will automatically be sent to the thieves, who then can make a fake credit card. Again, no manpower needs to be present at the point of sale; the thieves can remain in a remote area and harvest stolen data.

The massive dissemination of data made possible by the Internet and new media technologies has led to more effective police work. Rapid data collection and dissemination are important elements in the success of policing efforts such as CompStat. Information sharing between various components of the criminal justice community facilitates efficient law enforcement. Databases accessible by police officers across regions or countries can save a lot of time and resources, especially in the case of repeat offences or transborder crimes. Police officers only need to access a DNA database and perform some clicks to analyse whether a particular person can be linked to the crime scene. In the meantime, criminals also misuse the open networks for crime purposes. The Internet consists of countless databases of information covering practically any aspect of life and, as such, provides them with valuable information crucial to their criminal activities. Not only is this information cheap; it also does not require any particular skills to access it because it is mostly provided in a user-friendly manner. On the Internet, it is for example possible to obtain instructions on how to decode a digital rights management system for copyrighted works like DVDs, in order to convert them into downloadable files. These illegal copies will be distributed further, often commercially. Similarly, tutorials on how to write viruses are easily accessible in hacker sites on the Internet. Information on financial institutions, including their locations, pictures and design construction can be obtained electronically without having to manually survey those institutions. Criminals do not need to waste time, money or other resources in collecting information because a lot of information is just few clicks away.

2.1.2 International Cooperation and Networking

Changes in travel and technology have increased and altered the opportunities for seriously harming people and property in other national jurisdictions. Such transborder crime is certainly not a new phenomenon, and neither is international police cooperation to counter transborder crime. Police have long cooperated at the international level in investigating, prosecuting and securing convictions against persons involved in transborder crimes. Nevertheless, the advance of ICTs has simultaneously made transborder crime both more

prevalent and more serious. This situation calls out for, and has resulted in, more intense and improved cooperation between police services in different jurisdictions.[30] Coordinated efforts in international police cooperation can tackle transborder crime, which often works greater harm upon society than local criminality.

However, global networking is not exclusive to police, but is also engaged in by criminals. New technologies facilitate alliance and cooperation between criminals, and give rise to well-organised and large-scale transborder crimes such as money laundering, credit card forgery, trade in body parts and terrorism. Just like the police, the criminals share and exchange information with each other. They learn not only the potential, method and organisation of crime from each other, but also how to avoid crime detection. With global information systems, criminals can target thousands of victims in multiple jurisdictions per crime and, as a result, maximise the impact of their crimes.

2.2 Crime Race: Unwanted but Unavoidable

The foregoing has shown how ICTs can benefit criminals as much as the police. Criminals use ICTs to enhance their criminal activities, and police use ICTs to control crime. Ironically, perhaps, new technologies that facilitate crime control also accelerate the crime race. Both police and criminals race to use technology to outdo the other. At some points, it would seem that police and offenders are taking shifts in using a particular technology as the foundation for their next move. Invention of one technology is always followed by another invention, often as a counter mechanism to previous invention, as illustrated by following example.

After the instalment of speed cameras to catch speed offenders on the roads, the locations of speed cameras were compiled in databases. This data is now available for download to car navigation system with GPS. When approaching a speed camera, the driver will be notified, thus allowing him or her to adjust his or her speed and avoid being caught violating the speed limit. To counter this technology, another technology called the Speed Enforcement Camera System («SPECS») was developed to measure a car's speed between two cameras.[31] The system consists of a pair of cameras or more. The first camera reads the vehicle's registration number and digitally records the time

30 Anthony J. Blazer, International Police Cooperation: Opportunities and Obstacles, National Institute of Justice and National Criminal Justice Reference Service (US), 1996, available on http://ncjrs.gov/policing/int63.htm, last accessed 21 April 2008.

31 Detailed information on SPECS safety camera system is provided at http://www.speedcheck.co.uk/.

the vehicle passes that camera, while the second camera further down the road does the same thing. The system calculates the vehicle's average speed based on the time it takes to travel between the two cameras. By doing so, the system will be able to determine whether a certain vehicle was driven above the speed limit for that distance. A longer area of surveillance usually requires that more cameras be installed, although it is believed that they always operate in pairs, and not consecutively.

The development of interception and counter interception technology is also part of the race. First, communication technologies such as telephones, mobiles, radios and so on were invented to facilitate exchange of messages. Then tapping or interception was made possible by connecting a device to a telecommunication system that had the ability to record electromagnetic impulses as they passed along fixed wire telephone lines or radio frequencies. Before long, this was not considered to be enough. People wanted to *listen* as well as to record a conversation. The response to this demand was bugging technology. Now that computers are being used to exchange messages, technology for computer interception has joined the race. Miniature video cameras are custom-designed and installed in the computer to record images that actually appear on the screen. Another alternative, called computer eavesdropping, is facilitated by a scanner device that scans for electromagnetic radiation emitted from computers and converts this into visual images. To secure information and its transmission (including from interception), various technologies enabling data security, confidentiality and anonymity are also emerging. Encryption software, encrypted cellular phones and anonymous re-mailers that forward e-mails without revealing their origins are only a few examples of counter interception technologies. Not long after the appearance of these technologies, a stronger decryption algorithm was developed and threatened the security of encrypted messages. Interception technology is responded to with advanced counter-interception technology. Advance counter-interception technology is responded to with even more advanced interception technology. The race goes on. What is perhaps worrying is that police (for lawful purposes) and criminals (for illegal purposes) are *both* capable of exploiting these technologies in their operations. In practice, the decision to deploy any one of these technologies is often made based on an awareness of which technology is used by the opponent. The race is thus not only a technological race but also a crime race.

Technology can sometimes backfire on the police. When the police use technology to detect certain objects (weapon, illicit substances or drugs), smarter criminals may study the very same technology to avoid being caught or to develop other method of concealing weapons. Aware that DNA testing can

link a person to a crime scene, offenders learn to remove any DNA traces from the crime scene, and some even go as far as to leave other people's DNA samples to divert law enforcement attention from themselves. Such «offender learning», as Laylock pointed out, is a threat to the integrity of crime detection approaches.[32]

3 Societal Impacts

The role of ICTs in the context of crime control presents some notable implications for society in general. ICTs facilitate community education, influence behavioural change, and raise various public concerns while at the same time strengthening the impetus for law reform.

3.1 Public Concerns

Indeed, the Internet has become an invaluable tool in connecting community. It facilitates inexpensive mass community communication and education. Useful information, such as local crime trends, wanted criminals, missing children, drug abuse prevention, etc., can be passed to the community rapidly and continuously. Community members can learn about what, when and how a crime is committed in the neighbourhood and what actions should be taken in case of crime or other life threatening situations. Some police websites are equipped with interactive capability and allow visitors to send comments, feedback or tips to the police. This can help not only to control crime but also to improve community policing.

Despite these benefits, the Internet also presents dangers to society because there are no limits on the information available on the Internet. Practically any information can be found, including materials of illegal and sensitive nature. Some of the information may also conflict with other available data. Since it is impossible and impractical for the police to control access to all Internet sites containing illegal materials or access to highly protected materials, this information will continue to be available for anyone with access to Internet. This raises public concern as to the accuracy and integrity of information provided. Which site or information should the public trust? Anybody can provide information on the Internet, including people with malicious intentions; thus, the public can be wrongly informed. The Internet can also be used to spread fear, as has often been done by organized crime to intimidate anyone who may report organized crime-related activities or testify to a witnessed crime. As

32 Laylock, supra note 1, p. 48.

such, the flow of information, which can foster community confidence and the assurance of safety, depending on information provided, can also instil fear in communities and decrease respect for law enforcement.

Another concern is centred on the notion 'crime as opportunity'. Opportunities, which are often considered a «root cause of crime», play a role in causing all crime.[33] As technology opens easy opportunities for criminality, it also draws people into committing crime. Those people «become habituated to crime and always alert to criminal opportunities».[34] ICTs, especially the Internet, provide countless opportunities and methods for criminality. These include the opportunity to engage in both old and new forms of crime in a different and new environment. Electronic commerce made possible by the Internet in fact creates opportunities to practice cyber money laundering, cyber fraud and cyber terrorism. Reasonably, reducing opportunities means preventing crime. The question is how to reduce the numbers of opportunities offered by technologies in a modern society that relies heavily on these technologies to function? Increasing the risk of criminals being caught is perhaps one way of accomplishing this.

Implementation of ICTs may result in a change of behavioural pattern. Technology of surveillance such as video cameras, often created as a preventive measure, is actually a mechanism to induce conformity to expected behaviour patterns. Video surveillance is a form of behaviour control. Persons aware of being under surveillance are more likely to produce the peaceful social behaviour expected by society.[35] Thus, surveillance gives power to those behind the cameras in controlling the behaviour of people under watch. In modern cities where vast numbers of surveillance cameras are to be found almost everywhere, a person can end up under surveillance 24 hours a day. Complete surveillance can easily lead to a dictator-type situation where simply «watching» eventually turns into «dictating» behaviour.[36] This has raised the question of whether democracy is available for everyone, including for those whose movements are constantly being monitored.

---

33 M. Felson & Ronald.V. Clarke, «Opportunity Makes the Thief», Police Research Series Paper No. 98, Policing and Reducing Crime Unit, Development and Statistics Directorate (UK Home Office), 1998.

34 Ronald V. Clarke, «Technology, Criminology and Crime Science», European Journal on Criminal Policy and Research 10: 55–63, 2004, at p. 59.

35 See generally: Kathy G. Padgett, William D. Bales & Thomas G. Blomberg, «Under Surveillance: An Empirical Test of Effectiveness and Consequences of Electronic Monitoring», Criminology & Public Policy 5 (1): 61–91.

36 Federal Debt Relief System, Is Democracy for Everyone Where Surveillance Rules? Available on: http://www.fdrs.org/is_democracy_for_everyone.html#top, last accessed 21 April 2008.

The potential abuse of technologies raises the public concern that technology must be used appropriately and in legitimate circumstances. Technology of restraint, such as tear gas, while allowing officers to control riots in one area without using lethal force, can also be used for the purpose of punishment and torture. Technologies to detect hazardous or illicit substances concealed on the body, although meant for public security, bring up questions related to the right to privacy. As surveillance equipment becomes more sophisticated and available in many public spaces, concerns over individual privacy and freedom as well as the legitimate use of surveillance data are also emerging. Police ability to take and retain DNA samples from all arrested offenders (at least in the UK) can be seen as a serious infringement of human rights.[37]

There is also a concern about crime fighters' over-dependency on ICT. When police car patrol was first introduced, it was warmly welcomed, as it would help police to be more visible in the community. Experience shows that the computerized patrol cars tie police more to the vehicle rather than facilitating face to face interaction with community members. Therefore, any adoption of technology must be conducted with due care.

3.2 Regulation versus the Nature of Technology

Technological developments compel governments and law makers to be proactive in identifying the needs of their society. If citizens are to be protected from the adverse use of technology for criminal purposes, such an intention must be formalised in the laws. National laws need to be updated or replaced to deal with challenges posed by new technologies, in order to accommodate new criminal offences facilitated by ICTs. The problem is that ICTs change so fast that sometimes the law can not cope with their development. The law making process is usually long. On the other hand, new technological innovations are introduced to the society rapidly and continuously. Therefore, it is not surprising that the laws are often behind the technological inventions. Consequently, governments can be discouraged from updating the laws, choosing instead to allow private sectors to engage in self regulation.

In addition, the global nature of ICTs is a challenge for rigid regulation. Attempts to regulate the Internet have never been successful, especially when they are based on a fragmented approach. Given the inherent risk of the Internet in being misused for criminal purposes, the options of blocking access to certain Internet sites or controlling the content of Internet transmissions seems to be very appealing. However, not only is this is often technically

37 Laylock, supra note 1, p. 48.

impractical, but such regulation would also infringe on the fundamental right for freedom of information. Of course, governments and law makers have the right to prohibit certain contents or types of communications on the Internet but to expect those laws to be respected by all people around the globe with access to Internet is a vain hope.

Transborder crime calls for transborder measures. Internationally agreed upon and enforced laws secure broader implementation of the laws. Nevertheless, establishing new international legal instruments on ICTs is not an easy job due to the ever changing nature and vastness of ICTs. Up to now, no internationally recognised legal instrument regulates all aspect of ICTs. Indeed, some efforts have been made to harmonise national legislations against criminal use of ICTs. In Europe, such efforts resulted in the adoption of the Council of Europe (CoE)[38] Convention on Cybercrime of 2001 and its Additional Protocol of 2003. This Convention is the first multilateral treaty addressing criminal law and procedural aspects of various types of criminal offences against computer systems, data and networks. Before this Convention was adopted, member states of the European Union (EU) had ratified the EUROPOL[39] Convention of 1995, which, amongst other things, provided a framework for police cooperation against organized crime, including cyber crime. In 2005 the EU also adopted the Council Framework Decision 2005/222/JHA on Attacks against Information Systems, to approximate criminal law in the area of attacks against information systems. Other international bodies such as the United Nations and the OECD (Organization for Economic Cooperation and Development) also have addressed cyber crime. The United Nations adopted a *Plan of Action* dealing with the prevention and control of high-technology and computer-related crimes in 2001; and the OECD adopted *Guidelines on the Security of Information Systems and Networks* in 2002. These international efforts so far have touched the most critical issues raised by the use of ICTs to conduct crime, but much remains to be regulated in order to effectively addressing all aspects of ICT-related crime. Given that «the potential extent of computer crime is as broad as the extent of the international

38 The Council of Europe is the oldest international organisation working for the integration of Europe. It should not be mistaken with the European Union or its council, the Council of the European Union or the European Council. While the Council of Europe has a membership of 47 countries, the European Union has 27 member states. See http://www.coe.int/.

39 Europol (European Police Office) is the European Union's law enforcement organisation that handles criminal intelligence. It was founded to improve the effectiveness and co-operation between the European Union member states in preventing and combating serious international organised crime and terrorism. See http://www.europol.europa.eu/.

telecommunication systems,»[40] a common universal framework, that is not just regionally centred or organisationally exclusive, is called for. This should take the form of a binding legal instrument such as a convention on cyber crime under the auspices of the United Nations. Indeed, the CoE Convention on Cybercrime has so far been signed by several non-member states of the CoE such as Canada, Japan, South Africa and the US; but it is nonetheless a product of a regional organisation, which is based mostly on its members' premises and conditions.[41] On the other hand, a United Nations convention would be considered a joint product of its 192 member nations; and thus would arguably appeal to the international community.

Nevertheless, to come up with a universal convention is not an easy task. Not only it is difficult to set rules and policies common and acceptable to all nations, but even to agree on terminology has proved to be a problem. As mentioned earlier, many terms such as cyber crime, computer crime, computer-related crime, ICT-related crime and high technology crime have so far been used interchangeably to refer to the criminal use of ICTs; despite the fact these terms actually cover different crimes as well as «distinct factual situations».[42] Various international legal instruments in the field set different scopes in their definitions; and so far functional definitions have been the norm.[43] As an example, the CoE Convention on Cybercrime assumes cyber crime to involve the use of «computer networks and electronic information» for committing criminal offences,[44] and criminalises several categories of offences against computer systems, networks and computer data, as well as the misuse of such systems, networks and data.[45] One of these categories is «computer-related offences,» which covers computer-related forgery and computer-related fraud. On the other hand, Europol used the term «high technology crime» to refer to the use of «information and telecommunications technology» to commit or further

40 United Nations, «United Nations Manual on the Prevention and Control of Computer-related Crime,» International Review of Criminal Policy Nos. 43 and 44, available on http://www.uncjin.org/Documents/EighthCongress.html, last accessed 18 April 2008.

41 As of 24 April 2008, 44 countries have signed the CoE Convention on Cybercrime, and half of those signatories, including the US, also have ratified it. For a complete chart of signatures and ratifications, see: http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=4/22/2008&CL=ENG.

42 See generally: Fausto Pocar, «Defining Cyber-Crimes in International Legislation», European Journal on Criminal Policy and Research 10: 27–37, 2004.

43 See generally: United Nations Manual on the Prevention and Control of Computer-related Crime, supra note 40.

44 See Preamble of the CoE Convention on Cybercrime.

45 This includes offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences and offences related to infringements of copyright and related rights.

criminal offences against a person, property, organisation or network computer system. As part of this high technology crime, cyber crime is defined as «the criminal use of any computer network or system on the Internet; attacks or abuse against the systems and network or system on the Internet; attacks or abuse against the systems and networks for criminal purposes; crimes and abuse from either existing criminals using new technology; or new crimes that have developed with the growth of the Internet.»[46] The 2007 EU Commission Communication on *Towards a general policy on the fight against cyber crime*[47] also sets different scopes in its definition of cyber crime. In this Communication, the term cyber crime is applied to three categories of criminal activities: (i) traditional forms of crime such as fraud or forgery specifically committed over electronic communication networks and information systems, (ii) publication of illegal content over electronic media such as child sexual abuse material or incitement to racial hatred and (iii) crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking.

The above shows that activities included in the expression «cyber crime» can differ depending on legal instruments or organisations. This has led to difficulties in coordinating international actions against the criminal use of ICTs. Needless to say, it is crucial to the success of any international effort to combat transborder crime to have consensus on which term to use as well as its definition.

The nature of ICTs also presents difficulties for the implementation of criminal laws, especially in relation to the application of conservative rules and jurisdictions. It is well known that legal concepts of criminal laws were defined in relation to a particular jurisdiction or locality. For example, «theft» is normally defined as the removal or taking away of goods from their place. At the current time, information is valuable and prone to theft. However, when information is stolen or illegally acquired, there are no goods actually taken. In other words, there is no carrying away of property. Would this mean that a person stealing information is not punishable by criminal laws? Some countries, including the United States, have responded to this issue by passing a new law extending the

46 Dick Heimans, «Cybercrime – the EU Response», The IEEE Summit on Computing and Law, IEEE Computer Society, 2004, p. 91, available on http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1514379, last accessed 21 April 2008.

47 COM (2007) 267 final, 22.5.2007.

meaning of «property» to include information electronically processed or produced by a computer in either machine or human readable form.[48]

The territorial principle of criminal law is also challenged by the borderless nature of the Internet. Pocar noted that prosecuting and trying persons involve in cyber crime present difficulties in «the determination of the place where the offence was committed (*locus delicti*), to the application of *ne bis in idem* principles when several jurisdictions are equally competent, and to the avoidance of negative jurisdiction conflicts».[49] Not surprisingly, Pocar then suggested the use of the principle of universality, which is normally applicable to crimes against humanity, war crimes and genocide, as a ground for criminal jurisdiction. According to this principle, any nation is authorized to prosecute and punish violations of human rights wherever and whenever they may have occurred. Indeed, the chances that cyber crime would result in *serious* violations of human rights, such as war crimes and genocide, have so far been almost nonexistent because these crimes are not typically computer related. Nonetheless, given the borderless nature of ICTs, combined with their potential and continuing development, use of ICTs to commit (cyber) crimes against humanity is not impossible; and thus will accordingly justify the use of the universality principle as grounds for criminal jurisdiction.

Concluding Remarks

Technology is a democratic instrument. It can be exploited by anyone, regardless of who that person is or the motive or aim for the exploitation. New technologies, especially in the field of ICTs, have opened new doors and created new pitfalls for both criminals and law enforcement. They provide police with crime control tools and criminals with crime enhancing tools. Applied intelligently, technology can change and improve the practices of both the criminal and the crime fighter alike.

As new technologies facilitate traditional and new offences in a rapid manner of commission and with a vast area of impact, they also make police work ever more challenging. Police utilization of crime control technology may catch common offenders, but it also encourages highly intelligent criminals to push, often with force, for the development of more advanced (crime) technology to counter crime control technology. Limited police resources and funding

48 See e.g.: Illinois Compiled Statues, Computer Crime Prevention Law, Chapter 720, Criminal Offenses Criminal Code, Article 16D, Computer Crime; North Carolina General Statutes Section 14–453 (as amended in 2002); Minnesota Statues Section 609–87 Computer Crime; Alabama Computer Crime Act Section 13A-8–101.

49 Pocar, supra note 44, p. 36.

in combating the sheer number of high technology crimes, not surprisingly, will cause police to be left behind in the race against smarter criminals. It is also a known fact that it is often easier to find flaw in a system than to build a totally attack-proof system. Criminals are aware of this and always up to the challenge.

Indeed, new and reformed laws and regulations on an international level are crucial to combat crimes of worldwide dimension such as cyber crime. Such international legal frameworks should at least provide and maintain a precise definition of cyber crime; and thus accordingly harmonise different national legislations on the central prerequisite for criminal prosecution, i.e. the specific elements of cyber crimes. Providing and maintaining a legislative regulatory framework on the use of new technologies will also offer general and specific deterrent effects which will hopefully ensure that infringements of individual rights are kept to a minimum. Furthermore, although technology and the crime race are often triggered and escalated by technology, reliance on technology is perhaps still part of the solution. This means that it may be necessary to fight technology with technology. It may not be able to offer an answer as *why* crime is committed, but technology can show *how* crime is committed. The human quest to find the true cause of crime will never end because as Clarke noted: «our knowledge of the roots of criminality will always have to be updated as society changes» [50] and technology advances.

50 Clarke, supra note 36, p. 61.

TOOL-SUPPORTED LEGAL RISK MANAGEMENT: A ROADMAP*

Tobias Mahler

This paper discusses possible methods and tools for legal risk management. Risk management refers to coordinated activities to direct and control an organization with regard to risk. Risk management involves applying logical and systematic *methods* for identifying, analyzing and treating risk with any activity, process or project. *Legal risk management* focuses on the systematic identification, analysis and treatment of *legal risk*. The first part of the paper discusses how a legal analysis, for example of a contract's terms and conditions, can be carried out based a *method* that is compliant with key international risk management standards. The second part of the paper examines how IT *tools* could be used to (1) carry out a systematic risk management process and document its results, (2) support a legal risk analysis through the use of graphical models and (3) provide an integration between existing legal information systems and any risk analysis tools, (4) possibly using some elements of automation. The present roadmap is intended to facilitate a discussion about the goal of legal risk management, and an analysis of possible ways to reach this goal. The paper's central thesis is that structured risk management methods could be a supplement to existing legal methods. Any potential benefit of introducing such methods depends partly on the availability of adequate and usable IT tools.

I Introduction

In Richard Susskind's book *The Future of Law,*[1] the author predicts a paradigm shift in the approach to a legal problem from *problem solving* to *problem prevention:*

---

* This paper was presented at the conference «The future of ...», Conference on Law and Technology at the European University Institute, Florence on 28th of October, 2008.

1 Richard Susskind, The Future of Law, Clarendon, Oxford 1998, p. 290.

> *«While legal problem solving will not be eliminated in tomorrow's legal paradigm, it will nonetheless diminish markedly in significance. The emphasis will shift towards legal risk management supported by proactive facilities, which will be available in the form of legal information services and procedures. As citizen learn to seek legal guidance more regularly and far earlier than in the past, many potential legal difficulties will be dissolved before needing to be resolved. Where legal problems of today are often symptomatic of delayed legal input, earlier consultation should result in users understanding and identifying their risk and controlling them before any questions of escalation.»*

This paper presents a roadmap towards a tool-supported legal risk management. Imagine a future in which some lawyers are also seen as *legal risk managers* by their clients or employers. Such lawyers will specialize in the identification of legal risk, and will be experts in the structured assessment and treatment of risk in the legal context. Of course, legal risk management is only one out of several different legal services offered by lawyers. Those lawyers focusing on legal risk management will use specialized methods and software tools in their risk assessments.

The topic of the present paper is a set of potential future developments. However, I will seek to avoid making predictions. Of course, it is necessary to develop some assumptions about the future, but these are only extensions of current developments, without adding anything substantially new. Really new developments, and particularly discoveries, are unforeseeable for epistemic reasons.[2] The present roadmap[3] for legal risk management is by no means a deterministic prediction, but should rather be read as a discussion of goals and ways to attain these goals. This roadmap should be seen as a contribution to a discussion about future *directions*, rather than as a literal map which indicates the path itself. As Winston Churchill put it, plans are of little importance, but planning is essential. Planning views the future in a non-deterministic way, where we can influence central elements of future developments, despite the likely prospect that the plan itself may need to be adapted on the way.

---

2 See N. N. Taleb, The Black Swan: The Impact of the Highly Improbable, Random House, Inc., 2008.

3 See in general about technology roadmapping R. Phaal, C. J. P. Farrukh and D. R. Probert, «Technology roadmapping: A planning framework for evolution and revolution» Technological Forecasting & Social Change 71 (1-2) 5-26.

II Legal risk management

This section introduces legal risk management as the proposed goal for this roadmap. Legal risk management can be related to risk management in general. Risk management is today used in many different disciplines as a structured approach to deal with risk. Enterprise risk management focuses on risks to an enterprise. Financial risk management deals with risks, for example, in an investment portfolio. Engineers use risk analysis, for example, to analyze the risk of technical failure of a system. The characteristic element in *legal risk management* is the focus on legal issues in the context of risk. This legal perspective on risk becomes visible in the management of *legal risk*[4]. This perspective is in itself not new; practicing lawyers already deal with risks on a daily basis. The only proposed new elements are (1) the *conceptualization* of these activities as a type of risk management, (2) the search for more *structured methods* to carry out legal risk management tasks and (3) the possible development of *software-based tools* to support legal risk management.

The *conceptual question* is a contemporary, rather than a future issue. As Wahlgren[5] has indicated, some of the risk-related work tasks of practicing lawyers should be conceptualized as pertaining to the field of a risk management. According to the ISO, the term risk management refers to «coordinated activities to direct and control an organization with regard to risk».[6] By relating legal risk management to other risk management approaches, we may contribute to the development of a practical theory of proactive legal practice, which today is rather immature. There is an abundance of theory about how to interpret the law, once a problem arises. But legal theory has relatively little focus on how to avoid problems. Understanding and denoting some of lawyers' tasks as risk management provides us with a set of risk-related concepts and analyses, which may turn out to be helpful also for the analysis of legal risks.[7]

In my opinion, there are few alternatives to the conceptualization of lawyers' risk related tasks as legal risk management. When a lawyer analyzes potential risks (e.g., when drafting a contract), and how to avoid a negative outcome (e.g., when choosing the best wording for a contract), this may *also* be seen as *risk management*. However, the interesting question is not the conceptual or

4 Tobias Mahler, «Defining Legal Risk» S Nystén-Haarala (ed.) Corporate Contracting Capabilities: Conference proceedings and other writings University of Joensuu Publications in Law, Joensuu 2008, pp 51–76.

5 Peter Wahlgren, Juridisk riskanalys: mot en säkrare juridisk metod, Jure, Stockholm 2003.

6 ISO, Comittee Draft 2 for Risk management - vocabulary (Guide 73, 2008).

7 See further Tobias Mahler and Jon Bing, «Contractual Risk Management in an ICT Context -- Searching for a Possible Interface between Legal Methods and Risk Analysis» Scandinavian Studies in Law 49 339-358.

terminological issue of *whether* lawyers do risk management, but *how lawyers should manage risk*. The answer to this second question will be discussed in the remainder of this section. An analysis of legal risk management *methods* is a necessary basis for a discussion of possible legal risk management *tools*, which will follow in Section III.

A Legal risk management methods

Susskind's future of law predicts «legal risk management, supported by proactive facilities, which will be available in the form of legal information services and procedures». Could such *procedures* and *proactive facilities* for legal risk management be based on established risk management methods?

There have been some suggestions in legal literature to use formalized risk management approaches in law[8], but so far, legal risk management is, if anything, still emerging as a methodological approach. The goal for legal risk management is to facilitate the management of legal risk. While risk management also may be carried out informally, there may be some situations and contexts in which a more formalized risk management process and methods may be advisable. The term *method* is here used as a *codified set of recommended practices*. Interestingly, discussions of explicit practical proactive methods do not have a strong academic tradition in law. However, this does not necessarily indicate that a structured methodological approach is entirely irrelevant for or inapplicable to complex tasks typically carried out by lawyers. Rather, the lack of academic studies on practical methods seems to reflect the tradition of leaving the practical method to the legal practitioners. However, given the increased complexity of legal practice in a diversified international context, it may nevertheless be useful to devote some research effort to developing practical methods with clear interfaces to methods used in other disciplines.

1 Risk management

In general, risk management consists of one or more *risk assessments*. Typically, a risk assessment involves risk identification, risk estimation, risk evaluation and

8 See Katharine Reid, Risk-e-business: A framework for legal risk management developded through an analysis of selected legal risks in Internet Commerce (University of New South Wales 2000); Wahlgren, Juridisk riskanalys: mot en säkrare juridisk metod, above note 6; Petri Keskitalo, From assumptions to risk management: an analysis of risk management for changing circumstances in commercial contracts, especially in the Nordic countries: the theory of contractual risk management and the default norms of risk allocation, Kauppakaari, Helsinki 2000; Petri Keskitalo, «Contracts + Risks +Management = Contractual Riskmanagement?» Nordic Journal of Commercial Law [2006] (2) .

risk treatment. For example, a strongly simplified version of an engineering risk assessment may (1) identify the risk that a bridge collapses, because it cannot withhold an earthquake (risk identification). Then, (2) the engineer would analyze the uncertainty and assess the likelihood and the consequences of a bridge collapse due to an earthquake (risk estimation). The next step (3) would be to assess whether this risk is acceptable (risk evaluation). Depending on the evaluation results, the engineer would then (4) proceed to discuss the effect and cost of possible technical or other measures to manage the risk (risk treatment).

Could a similar approach be used to assess legal risk? This would require a risk assessment that not only focuses on factual events, but also on the application of legal norms to these facts. A legal risk assessment should assess how the application of legal norms may have an effect on the stakeholder.

I suggest as a starting point that a legal risk assessment should concentrate on the identification, estimation and treatment of legal risk. Thus, we need to clarify the meaning of the term «legal risk».

2 Legal risk

An obstacle is of course that there does not seem to be any agreement about the definition of legal risk in literature and practice.[9] In particular, it is not clear (1) whether legal risk implies that there must be uncertainty about the outcome and (2) whether this uncertainty must necessarily be legal uncertainty, or if uncertainty about facts is sufficient. For the purposes of this paper, I therefore suggest the following working definition of legal risk:

Legal risk refers to the risk of a future legal decision.

Two observations should be made with respect to this working definition. First, this definition does not focus on how legal risk is caused, but rather on how legal risk materialises (in a legal decision). Second, the definition depends on two other terms, namely «risk» and «legal decision», which both need to be clarified. There is no need to define risk differently than in other contexts, so I suggest we use the definition contained in the draft ISO risk management vocabulary.[10] There, risk is defined as the «effect of uncertainty on objectives.» The use of this definition in the context of legal risk thus implies that also legal risk must be an effect of uncertainty. Uncertainty is by the ISO defined as «state, even partial, of deficiency of information related to or understanding or knowledge of an event, its consequence or likelihood». An *event* is according

9 Mahler, «Defining Legal Risk» above note 5.

10 ISO, Comittee Draft 2 for Risk management - vocabulary above note 6.

to the ISO the occurrence or change of a particular set of circumstances. Note that this definition of events may be sufficiently broad to include legal decisions. Thus, in the context of legal risk, uncertainty could be the deficiency of information, understanding or knowledge of a legal decision, its consequences or likelihood. So now we need to introduce at least a preliminary definition of the term legal decision.

> *A «legal decision» is any type of decision that is (at least in part) based on legal norms.*

The term «legal decision», as it is introduced here, is meant to cover at least two types of rather distinct legal decisions. The *first* type of legal decisions is the *legally binding decision* by an actor who holds a particular legal power. The ideal type of the binding legal decision is of course a judge's judicial decision in a court case. However, other relevant decision-makers could be authorities or even a third parties, like a contract partner, who holds a particular legal power.

The second type of legal decision of relevance for legal risk is the decision which is taken by any actor *in light of the legal norms that apply to the decision*. This type of decision is much less formal and visible than the first type. The decision may not have to be conscious, and it may or may not even be easily discernible in the actor's behaviour.[11] This type of decision is not characterized by its bindingness (even though it is possible that the decision has certain binding effects on others), but rather through the direct effect the decision has on the actor's behaviour. One example of this type of decision is a *compliance decision*.[12] The compliance decision is taken by the complying actor, based on the identified set of norms that apply to the decision. An example is my decision to pay a certain sum of money to someone else, *because* I am obligated to do so. Another example of this type of legal decision is the decision to *bare a negative outcome*, without making any legal claim (e.g. for compensation). In both examples, the actor acknowledges the binding force of the legal norms.

11 The actor may (unconsciously) decide to do nothing. For example, an actor faced with an economic loss does not to make any claim, because no claim would have sufficient support in the law. It would be possible that the actor does not even think about the potential option of making a claim.

12 A relevant question is how we should deal with non-compliance. Most likely, non-compliance has a different place in the context of legal risk. Non-compliance may be one of the causes of a legal risk, but not of the consequences. However, this aspect must be left open for the time being.

For lack of a better name, such decisions will subsequently be referred to as the *actor's non-binding decision of its own affairs*.

We may ask why it is necessary to include this second type of legal decisions when identifying legal risk. Isn't it sufficient to focus on the binding decisions of judges, authorities and others? Doesn't the bindingness of these decisions represent the core element of the law, as a set of binding rules? The answer is a rather simple combination of empirical facts and pragmatic judgment. *First*, very few legal problems are ever brought to court. In most cases we either comply immediately, or after some negotiations, or simply do not comply with the law at all. This empirical fact needs to be taken into account when we identify how the law may have an effect on us in the future. *Second*, the actor's non-binding decision of its own affairs is included because its economic and other effects on the actor are to a certain degree comparable to binding legal decisions. From a practical perspective, I am affected both by a judicial decision which states that I have to pay a sum of money, and by my own decision to comply with my payment obligations. Of course, there are differences between the two types of decisions, and these should not be neglected. In particular, my own decision has surely an immediate effect on me, while a future judicial decision may be uncertain both in terms of whether I have to pay and how much I will have to pay. However, these differences do not justify omitting the second type of decision from our framework.

Instead, we should rather highlight how the two types of legal decisions are connected. Arguably, in most cases, the actor's non-binding decision about its own affairs is the only *real* decision, while the binding decision is only *hypothetical*.[13] An actor who decides to fulfil its obligations may or may not assess the hypothetical case that the problem is decided by e.g. a judge. If this assessment is made, then the result is likely to be one of the factors that contribute to the actor's decision of its own affairs.

In many other cases is a real binding decision, e.g. a court decision. In this case, the actor is forced to consider the effects of the binding decision, particularly in the light of a possible enforcement. If we assume that the binding decision itself does not directly initiate its own enforcement, then the actor is again faced with a decision of its own affairs, but this time the decision is about the actor's response to the decision. Thus, the actor's assessment of its options (including in particular to appeal, to do nothing, to await enforcement, or to comply) can again be characterized as the actor's decision of its own affairs. The important point is that both types of decisions may have an effect on the

13 Of course, at the time of the legal risk assessment (ex ante), both decisions are future decisions and thus to a certain degree hypothetical.

actor's objectives. This potential future effect is the key reason why legal decisions are of key relevance to a legal risk assessment.

3 Risk assessment method

A key difference between the example engineering risk assessment and a lawyer's risk assessment is that lawyers typically don't follow a standardized method. However, the following *typical practice* may be discerned by comparing the above procedure to the steps that arguably will be followed by many lawyers, when analyzing a future situation. Generally speaking, a lawyer might typically (1) identify risks, then (2) *analyse* how the relevant law (or contract) regulates the issue at stake (*hypothetical application of the law*), and then (3) evaluate whether the legal outcome serves the interests of the client and conclude by (4) proposing to *treat* the risk with adequate measures. These measures could then be implemented by the lawyer's client, based on an informal cost benefit assessment, which also takes the legal validity of the measures into account. The key difference between the lawyer's assessment and the engineer's risk assessment lies in the fact that the lawyer typically does *not estimate the risk value*, that is, the likelihood and consequences of the risk. At most, the hypothetical application of the law will include an *estimation of a likely legal output*, which depends on legal uncertainty.

Nevertheless, the above legal practice could be understood as a purely qualitative legal risk assessment method, which may be supported by some of the tools described in Section III. In addition, it might in some situations even be useful and cost efficient to go a step further and *estimate risk values*, as it is practised in other disciplines' risk management methods. In the following, I will exemplify how a full-scale semi-quantitative risk assessment method could be used to assess the clauses of a contract.[14]

B Example: contract risk assessment

The method discussed below is based on an adaptation of existing international standards for risk management to the requirements of a contract analysis. The relevant standards include the Australian Standard AS 4360/2004 and the currently available draft version of ISO standard 31000 «Risk management – Principles and guidelines on implementation». The process of risk management is a continuous process, which is carried out through *risk assessments*. If a contract is examined in a formalized risk assessment, then some of the steps specified in

14 This section is based Tobias Mahler, «How can we manage contractual risk?» Contracting Excellence [2008] 1 (5) 15-16.

the Australian Standard need to be adapted. This article may be complemented with literature on the use of the Australian Standard, which explains details of the general process, which cannot be sufficiently covered here.[15]

A contractual risk assessment can consist of the following steps:

- Specify the context, target and scope of the risk assessment (what exactly do you want to analyze?).
- Identify risk, that is, describe possible events and legal decisions, based on the contract clauses as applied to the contractual relation. Based on the contract clauses and the business context, what legal decisions may have an effect on the stakeholder?
- Estimate the likelihood and consequences (for example, monetary) of each identified risk. The estimation of likelihood should consider both the likelihood of facts and a relevant interpretation of the contract clauses.
- Evaluate the risks, distinguishing between acceptable risks and those risks that should be considered for treatment. This evaluation should be based on both the risk values (that is, high or low risk) and a suitable set of decision criteria.
- Consider how risks can be treated through practical measures or a suitable contract amendment.
- The decision about treatment implementation depends on a cost-benefit analysis.

Consider the following scenario. The management in an automotive supplier requests that a lawyer assess the general purchasing terms and conditions of a car manufacturer. Let us assume that the supplier's management has had positive experiences with risk management in other contexts, and suggests that the lawyer use a standard risk management method. The overall objective is to negotiate a side letter, containing more beneficial terms and conditions regarding those contract clauses that imply too much risk. As a preliminary step in preparing and negotiating this side letter, the lawyer has to clarify *how risk management can be applied to contract drafting*.

Again, the idea of relating contracting with risk management is in itself not new, but there is relatively little literature on how contractual risk management should be carried out in practice.[16] This Section attempts to propose some key

15 Standards Australia and Standards New Zealand, Legal risk management, Sydney 2007.

16 See in detail, Tobias Mahler, «The State of the Art of Contractual Risk Management Methodologies» H Haapio (ed) A Proactive Approach to Contracting and Law Turku University of Applied Sciences, Turku 2008, p. 58–72.

elements of such a method. The method has been applied in practical case studies, including the above-mentioned scenario, and is currently under evaluation.

1 Context, target and scope

Every risk assessment should start with specifying its exact scope and target, which in our context needs to be related to the rules in a contract. Depending on the time available and the importance of certain issues, the risk assessment could *target* the whole contract or selected parts of it. Of course, if parts of the contract are excluded from the formal risk assessment, they should still be assessed less formally outside the risk assessment. The *scope* of the assessment depends on the client's requirements to cover, for example, certain types of risks or to analyze a particular set of documents. It may be necessary to spend some time on establishing the *context* and describing what the contract aims to regulate. Preferably, this background information should be well-documented and available for review during the remaining assessment.

The quality of the risk assessment results depends to a large extent on the available experience about, and knowledge of, the domain in question. Typically, few individuals have a comprehensive understanding of all relevant aspects of a complex business contract. A lawyer is competent to analyze the contract clauses, but often lacks detailed operational knowledge. Similarly, technical experts may lack detailed information about financial and legal consequences of technical problems. For complex commercial contracts it may therefore be advisable to carry out a contractual risk assessment with a suitable *inter-disciplinary team* of *experts*, covering, for example, legal, financial, technical, market and other perspectives. A lawyer with experience in risk management could lead the assessment if the main focus is on legal aspects.

Every risk analysis focuses on identifying events (including legal decisions) that may impact the client's objectives or key assets. Therefore, the assessment should specify what the client wishes to protect, by listing relevant *objectives* (including the protection of its *assets*). It is also useful to initially set out how risk will be documented and measured (for example, quantitative or qualitative *risk values*) and what *criteria* for risk evaluation the client wishes to use. Guidance on the latter questions is available, for example, in literature on the use of the Australian Standard for risk management.

2 Risk identification

The second step consists in identifying the risks. In general, this involves identifying what, why, where, when and how *events* could impact the achievement of the organization's objectives or the value of its assets. In the context of a contract draft, we are particularly interested in legal decisions that are based

on the contract text. Therefore, one possibility for risk identification is to analyze one clause at a time, seeking to find out *how each clause could lead to a legal decision that impacts the organization's objectives or assets*. In practice, this involves brainstorming about likely facts and subsequent decisions that could negatively impact the client's objectives. In this context, the risk identification also needs to consider the *interplay between different contract rules rules,* which may be relevant for a legal decision. For many decisions, several clauses need to be read in a suitable combination. For example, the contract may include a 'time is of the essence' clause, implying several risks for the supplier, including liability for damages in case of delay. In order to assess the risk, the analysis also needs to contain what impact the applicable law and other relevant material may have on the rights and duties of the contract parties. The outcome of this step is a list and a description of possible legal decisions, which should include a description of both the anticipated facts and the anticipated legal assessment thereof. This list may consist both of binding decisions by e.g. courts or other authorities, and of the actor's own non-binding decisions of its own affairs, in recognition of the legal norms included in the contract or in the background law.

3 Risk estimation and evaluation

The analysis should subsequently make an effort to estimate the likelihood and consequence values for all identified legal decisions. The *consequence* value is an estimation, for example, of the monetary consequence, of the legal decision. The *likelihood* value is an estimation of the frequency or probability of the decision. The likelihood of the decision may directly depend on the rules contained in the contract. Because the interpretation of the rules is not always certain, this uncertainty should be directly included in the analysis. The likelihood of the legal decision may thus depend on *likely facts* and a *likely interpretation of the contract*. For example, the analysis can combine the assessment of the *factual* likelihood of a delay with an estimation of the *legal* likelihood of a particular contract interpretation that implies a payment obligation in case of delay. Thus, if it is unlikely that the contract can be interpreted to the effect that the client has to pay damages for delay, then the likelihood value is lower.

The combination of *likelihood* and *consequence* values renders the risk value, according to which the analyst can prioritize the risks. Subsequently, the team should *evaluate* which risks can be accepted, for example based on their low risk value, and which need be considered for treatment. This evaluation should be based on the client's risk appetite, the balance of risks and benefits in

the contract, and other criteria, for example, including the degree of influence the client has on the manifestation of the event.

4 Risk treatment and cost-benefit

The final phase focuses on how the identified risks can be treated. There are two key types of treatment of particular relevance to contracts. First, the risk may be treated by *practical measures* that ensure that a particular legal decision is less likely to happen, or less costly. Second, it may be possible to amend *amended certain contract clauses during contract negotiation*. For example, if the contract includes the clause 'time is of the essence' and the risk analysis team considers that there is a risk that the supplier will have to pay a substantial sum of damages for delay, then the treatment options include both contract amendment (for example, deletion of this clause or limitation of liability) and practical measures to reduce the likelihood of delays. The choice among the treatment options depends on a *cost-benefit analysis*. The benefit corresponds to the anticipated effect of the treatment on the risk level. This benefit needs to be related to the estimated cost of implementing the treatment. The cost-benefit analysis thus results in a recommendation of actions to manage the identified risks that can be presented to the decision-maker.

C A methodological supplement

It is difficult to anticipate the potential role of the above introduced approach within the portfolio of proactive legal methods available to lawyers. Today, there is no standard way of analyzing risk in a legal context.[17] While engineers, IT security experts and enterprise risk managers increasingly use standardized assessment methods, we lawyers seem to use experience-based heuristics to manage complexity and risk. This established approach has worked well in the past, and we should be very cautious about replacing it. In fact, given the immaturity of methods for legal risk management, it is so far not a realistic alternative for most of the daily practice of practising lawyers. Structured legal risk management should *not replace* existing legal methods, but it could support and accompany existing approaches as a supplementary method. The above described semi-quantitative method for contract risk assessment could be used in a situation where:

- there is a need or desire to get a more comprehensive and detailed understanding of the risks inherent in a contract compared to a traditional non-formalized analysis;

17 Ibid, p. 58–72.

- the contract text is stable during a sufficient time to carry out the analysis; and
- sufficient time is available for a detailed assessment — the necessary time depends on how selectively the assessment scope is chosen, but the required time for a detailed risk assessment could easily be several times the duration of a traditional contract analysis.

Legal risk management methods may be used for other purposes than contract analysis, too. There are several incentives to adopt a structured approach to legal risk management. For example, in an enterprise risk management (ERM) assessment, the general counsel of a company may be asked to identify and estimate risks within his or her field of responsibility. In this case, the general counsel would need to follow the established ERM method to identify and estimate risk. The need for a sufficient overall risk management in a company may subsequently require the law department to identify and estimate risk in their daily practice, in order to be able to report consistently. The dynamics of the largely soft-law based trend to ERM and its implications for legal practice is difficult to anticipate. In some countries, including e.g. Germany, some companies are already by law required to have consistent ERM systems, and such requirements could be extended in the future.

Similarly, a systematic approach to risk management may be requested by customers of legal services. For example the handbook for legal risk management, issued by Standards Australia and Standards New Zealand, encourages its readers to request that their legal advisors follow a systematic risk management approach.[18]

However, a key problem with risk management is that it is rather time-consuming and complex. Therefore, any success of the methodological approach will lastly depend on an adequate tool support.

III Tools for legal risk management

Enterprise risk management and financial risk management are carried out differently, and are supported by specialized tools. The same would have to be true for legal risk management.

How could the above introduced method for risk management be supported by tools? I will propose three complementary approaches, which could be implemented in combination or separately. The three approaches follow naturally from the risk management method. The keywords are (1) legal risk man-

18 Standards Australia and Standards New Zealand, Legal risk management, Sydney 2007.

agement *procedures and process*, (2) support for the difficult tasks of risk identification and estimation, which may involve communication between lawyers and non-lawyers and (3) the implementation within, or interoperability with, existing legal information systems. Moreover, all three types of tools or systems may in addition cautiously introduce selected elements of automation.

A Legal risk management process and administration

Tools that structure, simplify and facilitate a coherent analysis are often used to support risk management in other fields. Typically, risk managers need to capture and document the identified risks, their values and potential treatments. These administrative functions are already available in existing risk assessment tools. A good risk assessment tool assists the risk analyst in carrying out the relevant analysis steps in a suitable order, and helps documenting all results in a consistent way, ideally in a re-usable fashion. However, existing tools are insufficient in a legal context, because legal aspects are typically not adequately integrated in these analyses. Moreover, most risk assessment tools are discipline specific and focus on financial, technical or other issues. Nevertheless, tools from other disciplines might be adapted to support legal risk assessments.

B Graphical tools to support risk identification and assessment

The second type of tools is likely to be more challenging than the above process and administration tools. Risk analyses often involve brain-storming activities in interdisciplinary groups of experts (so-called 'Haz-Ops'). This part of risk analyses is often rather difficult, because it requires the intellectually challenging discussion of probabilities that may lead to an event. It is arguably even more difficult, if the risk estimation is not limited to the likelihood of «facts», but also includes the likelihood of «legal outcomes».

For example, imagine a company that wishes to assess the risk that a particular technical failure leads to liability according to the clauses of a major contract, in the context of the applicable background law. In this example, an engineer would be able to estimate the likelihood of the technical failure, and a lawyer may need to be consulted when the legal consequences are assessed. In the same example, the risk analysis might also need to assess the legal and contractual consequences of market changes, e.g. major raw material price increases. In this case, it would be useful to convene lawyers, engineers and managers together, in order to discuss and estimate the risk consistently. This evidently requires communication and mutual understanding of the others'

disciplinary perspectives. Of course, such communication already happens, and is often successful. However, sometimes such communication may be challenging due to the different methods and concepts used by the different disciplines. Just imagine a meeting where the lawyer brings to the meeting the customer's general terms and conditions of purchase, under which the product will be supplied (45 pages), together with a book about the applicable law. The manager or the chief risk officer presents a set of spread sheets with financial information and risk estimates. The engineer contributes with a set of technical drawings and the results of the engineering risk analysis (e.g. FMEA, failure modes and effects analysis). Such an imaginary, but not unrealistic, meeting illustrates the clash of intellectual concepts behind the different disciplines which need to participate in the risk assessment.

It is my (unverified) impression from talking to managers and engineers in several companies is that *such meetings often do not happen* at all. Instead, the manager would at best send an e-mail to the lawyer, who then assesses the contract separately, with limited or no regard to the business and technical issues at stake.[19] At worst, the lawyer will not at all be consulted by the decision maker, for example to avoid a delay in the contracting process, or in anticipation of an incomprehensible and lengthy legalese statement, which is not at all related to the technical and business issues at stake.

This *communications problem* may be amongst the *causes* for Susskind's observation that «legal problems of today are often symptomatic of delayed legal input». Susskind assumes that «earlier consultation should result in users understanding and identifying their risk and controlling them before any question of escalation.» However, if communications problems are amongst the causes for *delaying* legal input, then these communication problems may need to be addressed by lawyers and their customers or colleagues. The difficult communication about identified risks, their estimation and treatment, needs to be supported by a number of complementary approaches, including education, improved internal culture in an enterprise and, possibly, IT tools.

Tools for communication support should of course be inspired by solutions that have proved successful in other disciplines. In computer science, graphical models are often used in systems design and analysis to illustrate the intended functions of the IT system. The Unified Modelling Language (UML) is a graphical language for visualizing, specifying, constructing, and docu-

19 Such an assessment is likely to follow the traditional method as introduced above, in the introduction to section II.A. This may, of course, be sufficient for standard cases. However, if the issues are complicated and the law department or law firm has little experience with this type of business, more communication may be necessary.

menting the artefacts of a software-intensive system. According to Wikipedia, the Unified Modelling Language offers a standard way to write a system's blueprints, including conceptual aspects such as business processes and system functions as well as concrete features such as programming language statements, database schemas, and reusable software components.[20]

Visualization is an interesting approach in the legal context, because some of the problems outlined above are not that different from the underlying analytical challenges of IT systems development, despite the obvious differences. IT systems development needs to deal with complex technical issues related to hardware and software, and the end product is essentially code, which may be unreadable for humans. This code has a mathematical and logical basis, but what counts is ultimately whether the IT system fulfils the users' requirements, i.e. whether the system works for and with human beings. The latter aspect is captured best in graphical models, which can be understood by the non-experts who participate in the specification of the system requirements. Since the code may be illegible, one uses simple graphics to facilitate an informed decision-making during systems development.

Code is not an unknown concept for lawyers, as observed by Lawrence Lessig,[21] who refers to laws as «east coast code» and to technology as «west coast code». However, problems with the readability and understandability of code are treated rather differently in computer science and in law. This is obviously partly related to the fact that source code is not written in natural language and thus may be both *highly complex* and *very difficult to read*, while legal texts do use natural language. Legal texts may be *difficult* to understand for the inexperienced, but they should normally not be completely incomprehensible (even though there are sufficient examples of incomprehensible legalese nonsense). Moreover, it cannot be neglected that understandability problems arise for completely different reasons. In most cases, «legalese» is used as a matter of tradition, and legal terms are used because of their specific legal meaning in the relevant legal community (as a *terminus technicus*). However, in some cases, the use of excessive legalese may even be employed as a strategy to inhibit the other party from understanding and appreciating its risks. In any case, legal work also has to face the problem of code which is difficult to read, understand and evaluate from the perspective of risk. Nevertheless, lawyers have traditionally been reluctant to introduce (standardized) graphical models to understand, analyze and manage complex legal issues. This may have many reasons, not least the lack of availability of such graphical models. However,

20 For an introduction to the UML, see www.wikipedia.org.
21 Lawrence Lessig, Code version 2.0, Basic Books, New York 2006.

in addition there may be some underlying problems that could inhibit a modelling approach. Again, the *qualitative perspective* in legal reasoning may make it difficult to press law and justice into formalized and partly quantitative models. Nevertheless, we cannot assess the potentials and limitations of graphical modelling for legal risk management before we have developed and tested it.

In risk management, there is also an extensive use of graphical visualization methods to support risk assessments. For example, fault trees or Bayesian networks can be used to estimate the likelihood of a risk event. Computer scientists have also developed their own models, inspired by the UML.[22] The graphical models used here are based on the above introduced concepts of legal risk management, which are an extension of the ISO vocabulary for risk management.[23] This is illustrated in the preliminary notation in Figure 1.

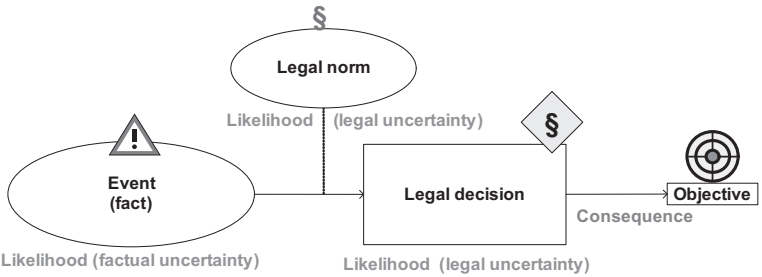


Figure 1 – Modelling legal risk

An example of a simplified legal risk diagram regarding a decision about a contractual obligation to pay consequential damages is provided in Figure 2 below. The diagram is meant to illustrate the following risk. In the unlikely event that a delivery is sufficiently delayed to result in loss of profit on the part of Buyer, Seller may decide to pay damages. The payment of damages is based on the contractual obligation to pay consequential damages, including loss of profit in cases of delay. The monetary consequences of the decision (a moderate consequence on the profits from this sale) are a result of the identified factual event and the application of the legal norm to these facts. The likeli-

22 Fredrik Vraalsen, Tobias Mahler et al., «Assessing Enterprise Risk Level: The CORAS Approach» D Khadraoui and F Herrmann (eds) Advances in Enterprise Information Technology Security Information Science Reference, Hershey, New York 2007.

23 This paper is based on draft risk management vocabulary, see ISO, Comittee Draft 2 for Risk management - vocabulary footnote 6. The latter was chosen, rather than the currently valid version (ISO 2002), because it is likely that this draft will be adopted in the near future. Implicitly, I accept the risk that the ISO may deliberate differently.

hood of the decision depends on the likelihood of the initiating factual event, plus the assessment of Seller's obligations in this event. The model in Figure 2 is simplified in order to illustrate the main features of the modelling approach. In particular, it would be possible to decompose the initiating event (by adding events further initiating events that contribute to the delay) and to add further consequential events and decisions.

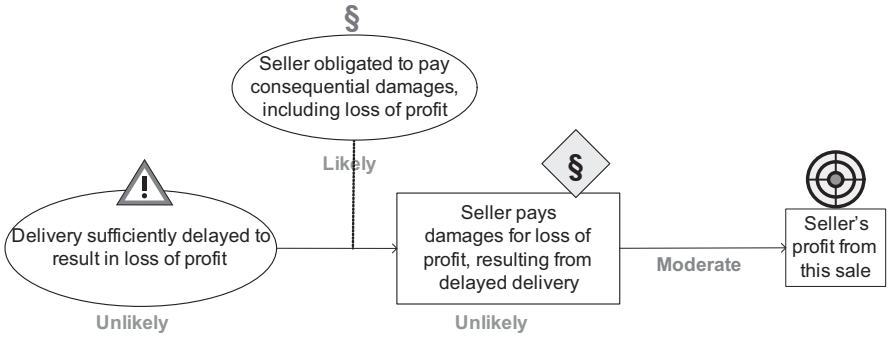


Figure 2 – The risk of obligation to pay damages for delayed delivery

The above examples are insufficient to appreciate whether the preliminary graphical modelling language as such is useful. However, the diagrams are here only included as *examples* of graphical models that could support a legal risk assessment. This is a tentative suggestion rather than the comprehensive solution to our problem.

This modelling approach is intended for the type of interdisciplinary legal risk assessment meeting described above. A previous (and more complex) version of the graphical language was tested in a full-scale industrial case study. Of course, the models imply a significant need for simplification, and the risk of over-simplification. However, this is a necessary consequence of introducing a model. If our limited brain resources could deal with all aspects of the complex reality, both today and in the future, then there would be no need for modelling.

However, since we have to take bounded rationality[24] into account, some degree of selective simplification may in some situations be better communication than the full complexity of lengthy legalese documents. In any case, graphical models are not necessarily intended instead of detailed legal analyses, but rather as an additional instrument to communicate a summarized result. If the output of a legal analysis is summarized in a concrete statement about risk and available options to manage such risk, then this output may be better understood and more easily used and implemented by non-lawyers. A suitable graphical legal risk management tool could therefore provide a simpler interface between the legal analyses and the risk analyses carried elsewhere in the organization. Graphical models alone will not solve the problem of delayed legal input, but if successful; they may be amongst the measures that can partly solve some of the communication difficulties during legal risk identification and assessment. This again might contribute to an increased and earlier consultation of lawyers, as intended by Susskind.

C Risk management and legal information systems

Ideally, any tool support for legal risk management should be integrated or interoperable with an available legal information system. Today, these include at least (1) legal information systems and (2) contract management systems.

First, law firms and law departments use a variety of legal information systems to retrieve legal information like statutory or case law, soft law (codes of conduct), contract templates and legal literature. Some systems already include a limited functionality for contract drafting, based on contact templates. Moreover, some of these systems already include modules which bare the title «legal risk management». The latter typically includes check-lists or similar tools to support day to day legal work. One example of a risk assessment tool is a German tool on a set of CDs entitled «tool-box of international trade law», where the user of the «risk analysis tool» can retrieve information about particular legal questions relevant to international trade law, with respect to a

24 The concept of bounded rationality is used to question the assumption, made in traditional economics and other sciences, that humans can be reasonably described as «rational» entities (for example in rational choice theory). Instead, bounded rationality theory seeks to account for the fact that perfectly rational decisions are often not feasible in practice due to the finite computational resources available for making them. This has also consequences for the way risks can be analyzed and described. For example, a recent article describes the communications problems when discussing medical risk assessments, and discusses ways for simplified and still correct presentation of a medical doctor's risk estimates, see Gerd Gigerenzer and Adrian Edwards, «Simple tools for understanding risks: from innumeracy to insight», BMJ 2003; 327:741–744, doi: 10.1136/bmj.327.7417.741.

number of jurisdictions.[25] This type of tool may thus be used to estimate the legal outcome of a standardized set of facts, which are relevant in international trade. However, the tool only focuses on providing rather limited information and thus only covers a minor part of the overall risk management process, and does not offer any support for risk estimation and evaluation in general. Nevertheless, legal risk management tools could in the future be integrated or made interoperable with relevant legal information systems.

The second type of system, which could be a candidate environment for legal risk management tools, could be contract management systems. In general, contract management is the administration of an organisation's contracts. Contract management includes negotiating the terms and conditions in contracts and ensuring compliance with these, as well as documenting and agreeing any changes that may arise during its implementation or execution. Today, contract management is in many organisations still carried out in manual processes without dedicated systems. However, e-mail negotiations and paper archiving routines often lead to poor availability of contracts in an organisation. Contract management software promises to solve this problem. Contract management software is intended to support contract creation, to ensure the availability of contracts and to support contract analysis. There are different approaches to contract management, but most contract management systems today allow a selected number of users to upload and change contracts, which then are made available for other users in the company. Currently, contract management systems seem to provide limited support for risk assessment. However, in the future, contract management systems could and should consider adding such functionality. The contract management system could, for example, assist in assessing the risk in a particular contract text that was uploaded into the database. Moreover, once the risk is identified and assessed, the results of the risk assessment could be used as meta information about the contract, which is documented and available for future reporting and other use. The identified risks may thus be monitored adequately. The identified risk may also be relevant for the analysis of other comparable contracts, where similar risks could be identified. Thus, it could become possible to consistently manage the risk in a portfolio of contracts.

25 Verweyen, Foerster and Toufar, Tool-Box des Internationalen Warenkaufs UN-Kaufrecht (CISG), 2008.

D A cautious approach towards automation

Lastly, it may be possible to cautiously introduce selected elements of automation into legal risk management systems. So far, the use of so-called expert systems and the use of artificial intelligence in law may not have been as successful and relevant as anticipated. However, given the fact that we still may be in the very early phases of IT development, this is not a sufficient argument to reject automation as such. A cautious approach to automation could imply the use of text parsers, e.g. to select rules that may be a source of legal risk. For example, the graphical modelling approach presented above distinguishes between obligations, prohibitions, permissions, legal qualifications and legal power. These notions play an important role in the modelling approach outlined above, as each of these notions has a distinctive effect on risk. There are readily available parsers that can identify such notions, and these seem to work even for languages other than English.[26] One option for automation could thus be that a tool extracted some of the conceptual notions in legal texts, and made the result available as a text paste option in a tool based on the above outlined graphical approach. Thus, the text «Seller obligated to pay consequential damages, including loss of profit» in Figure 2 could be extracted from the contract document, identified as an obligation and suggested as a text paste option in the diagram. This could safe some time and could improve consistency. Moreover, this could solve a problem in the current modelling approach, namely that different norms in one diagram could have different sources of law, which is difficult to visualize consistently in the diagram, but which could be made available as a link to the original source in the meta information for the diagram.

IV Outlook

Although there are a number of potential benefits to be obtained through the introduction and use of methods and tools for legal risk management, we need to acknowledge the significant difficulties and obstacles.[27] For one, lawyers are not trained in risk management methods, and are used to a substantial methodological freedom for all tasks outside the interpretation of the law. Moreover, law is often open to interpretation and legal decisions are not always predictable from the outset, so most legal risk assessments need to deal with rather

26 C. Biagioli , E. Francesconi , A. Passerini , S. Montemagni , C. Soria, «Automatic semantics extraction in law documents», Proceedings of the 10th international conference on Artificial intelligence and law, June 06–11, 2005, Bologna, Italy.

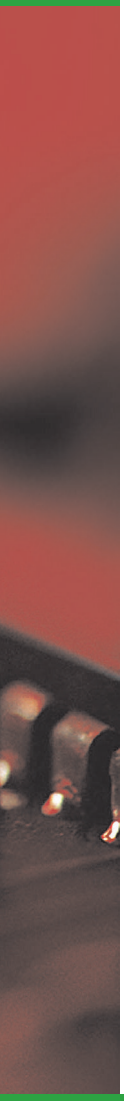
27 See also Wahlgren, Juridisk riskanalys: mot en säkrare juridisk metod, pp. 133–145.

uncertain assessments. Legal risk assessments may, in addition, be rather time-consuming and costly. Consider, for example, the possibilities of failure in a major commercial contract. The consistent analysis of all risks may be more costly than the potential improvement of the contract, if any, based on a more complete risk analysis. Therefore, it may only be cost-efficient to carry out a full scale risk assessment for contracts that either have an exceptional value, or that are sufficiently representative for other, similar contracts, so that the risk analysis results also are useful for those contracts that are not analyzed in detail. Last not least, clients may be less interested in paying expensive lawyers for a proactive legal risk assessment, compared to a situation in which a risk has already materialized and they necessarily have to face a major and costly legal problem. As a business model, legal risk assessment may therefore have some limitations for law firms.

These obstacles and limitations need to be taken into account in any development of legal risk management methods and tools. Nevertheless, there is sufficient potential in legal risk management to justify further research. The real benefit of new methods and tools for legal risk management can only be verified by defining a method for legal risk assessment, together with initial tool-support, and testing these in a suitable case study.

V Acknowledgements

The work presented in this paper was kindly financed by the Norwegian Research Council under the ENFORCE project grant.



Hvert år oppfordrer vi våre forskere til å gi bort en artikkel til jul. Dette er åttende gang Yulex blir sendt ut som julehilsen. Som tidligere år har også årets bok blitt en forundringspakke med varierte og noen ganger overraskende bidrag som vi håper leserne får glede av.

Every year we ask our researchers to write an article for Christmas. This is the eighth time we send Yulex as a seasonal greeting to our many partners and contacts. As with previous years, this collection of articles covers a wide variety of topics and may even contain a few surprises.

- Kven skal trøyste Hypomone? Eit kammerspel i tre akter om vern av pasientopplysningar
- Let there be LITE: A brief history of legal information retrieval
- Beskyttelsen mot overvåkning i den fysiske og elektroniske verden
- Personvernøkende teknologi og identitetsforvaltning
- Rational Concerns about Biometric Technology: Security and Privacy
- Når Høyesterett ikke finner loven
- Regulering av e-post som bevis etter den nye tvisteloven - praktiske og rettslige utfordringer
- How can ICT reform public agencies?
- Systemutvikling i rettslig perspektiv
- Bibliotekvederlaget
- Taking Advantage of New Technologies: For and Against Crime
- A roadmap towards Tool-supported Legal Risk Management

ISBN 978-82-7226-188-3