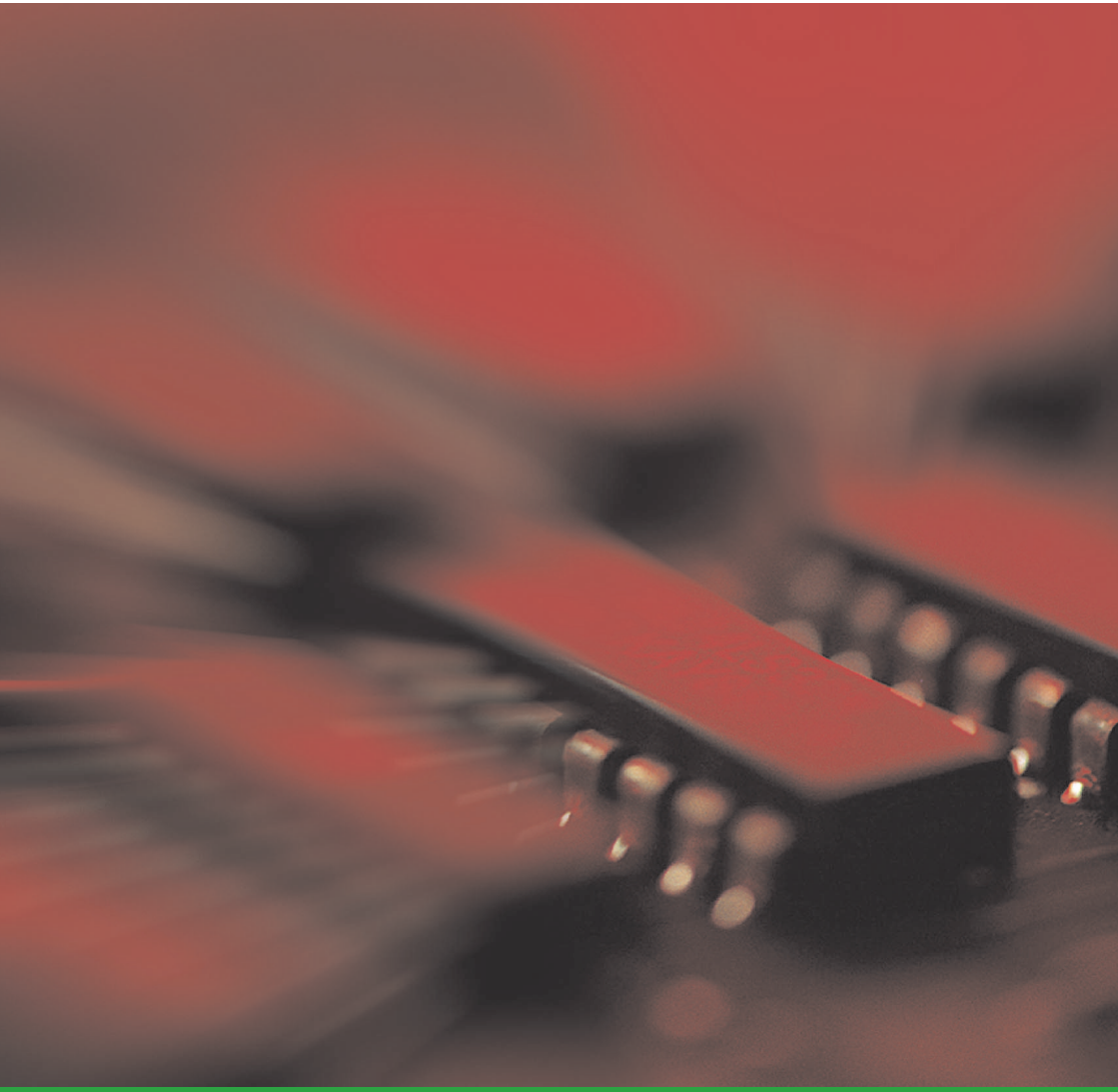
Dag Wiese Schartum og Anne Gunn B. Bekken (red.)

YULEX 2007



Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

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

YULEX 2007

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 978-82-7226-107-7
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

INNHOLD/CONTENTS

FORORD

Hvert år oppfordrer vi våre forskere til å gi bort en artikkel til jul. Hvert bidrag samles og pakkes inn i Yulex som vi sender som en julehilsen til våre mange samarbeidspartnere og kontakter. Som i tidligere år har også årets bok blitt en forundringspakke med varierte og noen ganger overraskende bidrag som vi håper du får glede av.

Ved utløpet av 2007 bestod Senter for rettsinformatikk (SERI) av i alt 31 forskere. Blant disse hadde 11 forskere sin primære tilknytning til andre instituttmiljøer ved Det juridiske fakultetet i Oslo, mens 20 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 nå sine mål.

Som resultat av overgangen til senter har vi dessuten fått en klarere tverrfaglig fagprofil en før. Selv om det juridiske perspektivet er og fortsatt vil bli dominerende, suppleres dette av en tydeligere informatisk og samfunnsvitenskapelig tilnærming enn tidligere. I tillegg favner vi vidt og er «tverrfaglige» også innen jussen i den forstand at de rettslige problemstillingene vi behandler omfatter privatrett og offentlig rett, og dessuten rettsspørsmål som vanskelig kan plasseres innen tradisjonelle kategorier. Denne boken viser litt av bredden.

God jul og god lesing!

FOREWORD

Every year we ask our researchers to write an article for Christmas. All of the contributions are collected together and form Yulex, which we send out 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. We hope you enjoy reading.

By the end of 2007, Norwegian Research Center for Computers and Law (NRCCL) had a total of 31 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 many 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.

In transitioning from an institute to a research center, our focus has become even more interdisciplinary. Allthough the legal perspective is and remains dominant, it will be enriched by a more pronounced informatic and social scientific approach. Moreover approaching legal problems we cross the traditional lines by making use of both public and private law as well as considering areas that are not easily placed in the traditional legal categories. This book demonstrates some of the breadth of our research.

Merry Christmas and enjoy!

FREMTIDEN PÅ SPILL

Jon Bing

Det sterkeste minnet fra mine barndoms somrer var en enkel lek. Sommerstedet vårt i Trøndelag lå ved bredden av en stor innsjø. Eiendommen var veiløs, og var sommerbeite for sau som hadde laget stier gjennom lyng og bregner. Skogen var for det meste gran og furu, med bjerk ned mot myrdrag og åpne glenner og selje i kratt langs bredden av vannet og den lille bekken fra den mørke tjønna. Selv nå, så mange år senere, kan jeg ikke skrive om dette uten å bli frustrert over hvordan jeg med ordene ikke klarer å presse frem den mystikken, de indre hemmelighetene som dette landskapet rommet. Betydningen av de ranke, høye furuene på en kolle over tjernet, som liksom skapte et rom av søyler og skrå knipper av lys, hvor storfugl ofte gjemte seg på toppen av noen mosegrodde kampesteiner. Eller den lille øya i bukten nedenfor husene som ble kalt Bismerholmen, og som vi visste – helt sikkert – at vikinger en gang hadde brukt som valplass for tvekamper der bare en forlot øya levende. Vi gravde under kreklingen etter bevis i form av pilespisser eller en spydodd, og fant mange overbevisende kandidater.

Det var i dette landskapet den store leken utspant seg, gjennom noe som for meg fremdeles står som en lang rekke somrer Det var ikke noe spesielt med denne leken, den var den samme som så mange barn i Norge har lekt under løvtrær og bak busker. Vi var indianere, selv var jeg Silver Horse, søsteren min var Golden Arrow. Vi hadde passende utstyr, spyd av rognekjepper, skjold av tønnebunner (mitt var malt med sølvmaling), fjærpynt med de vakre, blå fjærene til nøtteskrike … Venner var tilsvarende utstyrt.

Men det magiske var opplevelsen. For opplevelsen var ikke en lek, opplevelsen var et stort eventyr som utspant seg i de mektige skogene. Spenningen sitret gjennom oss der vi snek oss langs hemmelige stier i det landskapet vi kjente så godt, hvor luften var drektig av noe uforløst, hvor fargene var skarpe, lydene pregnante, hvor vi så forbi rekvisitter som tønnebunner og hjemmefargede trøyer med påsydde frynser til den indre virkeligheten, den vi skapte i vår egen fantasi – godt hjulpet av tingene vi hadde lånt fra hverdagen. Jeg kan huske det som smaken i munnen av noe søtt eller mettende som man dessverre har spist, og med tallerkenen tom foran seg.

Og grunnen til at jeg husker det så godt var den sommeren jeg mistet det. Den sommeren da jeg var blitt fjorten år, og full av forventning tok på meg indianerdrakten og gikk eventyret i møte. Noen timer var jeg del av hemmelighetene i opplevelsen. Men så falt jeg liksom ut. Jeg var bare en guttunge i fillete

klær med en kjepp i hånden. Jeg husker det så godt på grunn av min egen skuffelse og frustrasjon, ønsket om å dykke tilbake og ned i den felles opplevelsen sammen med søsteren min og vennene våre. Jeg klarte det av og til, timer av gangen, den sommeren. Men jeg visste at slike opplevelser nå var forbi.

Jeg var blitt for stor. Fjorten år gammel gråt jeg modige tårer over min egen tapte barndom.

Jeg har et beslektet barndomsminne. Spisebordet vårt hadde to plater som kunne legges i midten og slik gjøre bordet lengre hvis middagsgjester krevde det. Heldigvis var det sjelden. Derfor fikk søsteren min og jeg bruke platene som bunn i eventyrland som vi bygget av plastelina. Menneskene var små figurer mindre enn to centimeter høye, alt annet ble laget i samme skala. Vi brukte små glassdyr eller pappfigurer eller annet av riktig størrelse til å supplere landskapet, men det meste laget vi selv. To spisestuebordplater blir et ganske stort land i denne størrelsesordenen. Her laget vi eventyrriker – vanligvis ikke helt etter fritt skjønn. Vi tok gjerne utgangspunkt i en bok eller en serie med fortellinger. Barna i Nyskogen klarte seg på egen hånd lenge etter at forfatteren slapp tak i dem. Tarzan fant igjen sitt Afrika, Jukan sitt Amazonas, Hjortefot sine skoger …

Naturligvis var vi aldri del av fortellingen på samme måte som i sommerskogen. Vi var de som bestemte over hva som skulle skje, som fant på hvilke kriser som skulle ramme samfunnet, hvilke utfordringer heltene måtte løse – vi hadde regien, vi bestemte utviklingen. Det kunne ta uker å bygge ferdig et samfunn, og mange uker å leke seg gjennom mulighetene før det hele ble demontert, plastelinafigurene tatt fra hverandre, samme farge ble samlet i hver sin klump så det ikke skulle bli bare en stor, gråbrun masse igjen til neste gang et samfunn skulle konstrueres. Jeg husker spesielt en sjelden klatt med sterkt oransje plastelina som var kommet via en klassekamerat, og som jeg passet godt på så den ikke skulle bli «skitten».

Felles for disse eksemplene er to hovedtrekk. For det første friheten. Dette var lek uten andre regler enn vi laget selv. Men selvfølgelig var det regler, når man har frihet til å gjøre hva man vil – nedkalle lynild fra himmelen eller se gjennom tykke trær – da er det ikke morsomt uten at man har regler og begrensninger. Det vet alle som har prøvd.

For det andre rekvisittene. Den betydningen som holdepunkter hadde for fantasien. Vi forvekslet ikke en kjepp med et spyd, men spydet ble manet frem av kjeppen. Sammen med alt som hører med til et spyd – fjærdusker og jaktminner og krigsdanser … På samme måte som tynne plastelinaruller kunne

tegne omrisset av et hus, en borg, en labyrint – og de vokste opp av bordplatene – blinkende, forjettende og fulle av muligheter.

Når dette er sagt, er det lett å forstå at jeg er misunnelig på barn som vokser opp i dag.

Det er et ekko fra misunnelsen fra sommeren da jeg var fjorten år og innså at jeg hadde mistet evnen til å drukne i leken. For barn i dag har nesten immersive grensesnitt til lekens verden.

I 1982 – samme år som IBM solgte sin første «personal computer» – ble jeg bedt av OECD å skrive en artikkel om edb-spill.[1] Disse var i sin vorden, men jeg ga nokså hemningsløst uttrykk for min begeistring. Begeistringen hadde tynt grunnlag. Jeg hadde riktignok deltatt på turneringer i interaktiv tennis som ble arrangert av ungdommelige forskere i mitt eget miljø. Jeg tviler på at noen i dag klarer å opparbeide fascinasjon over to prikker («baller») som strengt følger reglene for at «innfallsvinkel er lik utfallsvinkel» der de tegner langsomme striper over en rektangulær bane. Og hvor man med fjernkontrollen kan flytte to racketer i form av streker for å intervenere og sende ballen i en ny retning. Men regler og teknologiens begrensninger var nok til å gjøre det til et spill sammen med pizza og øl. Selv om jeg ikke noen følelse av å spille på Wimbledon, så var det morsomt nok.

En helt annen opplevelse var erfaringene med interaktive romaner. Den første som fikk noen utbredelse i Norge, ble spilt på Universitetet i Oslos sentrale DEC-10 anlegg. Dette var et spill med et tekstuelt grensesnitt, som en vanlig bok. Men teksten sluttet plutselig, og fortellingen stanset opp. Da måtte leseren gripe fatt i hovedpersonen og foreslå hva som nå skulle skje. Slik ble fortellingen til i samarbeid mellom spillets regler og leserens fantasi.

Det kom en hel mengde slike interaktive romaner. En av de jeg husker best, var Trinity.[2] En situasjon der kan kanskje forklare noe av fascinasjonen. Hovedpersonen befinner seg i Kensington Gardens en ettermiddag da denne parken er – som vi alle vet – fylt av barnepiker med barnevogner. Det er lek langs stiene, noen vogner står tomme mens barnepikene steller med smårollingene. Det blåster i sterke vindkast, og noen av barnepikene slår opp paraplyer som rivers bort av vinden. Hovedpersonen vet at han (eller hun) må komme seg over plenen og ned til sjøen midt i parken. Det er bare det at når man skritter ut på plenen – der advarende skilt sier «Trå ikke på gresset» – så fanges anklene av strå som slynger seg rundt dem og gjør det umulig å komme videre.

1 Artikkelen er trykt i Impact 4/1982:425-431«The electronic game gambit».
2 **Infocom 1986.**

Løsningen? Det ligger en forlatt ball på en av grusgangene, det får hovedpersonen vite ved å «se seg om», det vil si at han eller hun ber spillet beskrive hvordan det ser ut rundt seg. Han eller hun tar ballen og kaster den mot en paraply som er fanget i en trekrone. Paraplyen faller ned, hovedpersonen setter seg opp i en av de forlatte barnevognene, slår opp paraplyen – og vinden kommer gufsende og fører den improviserte seilfarkosten over gressplenen og ned til vannet.

Gir dette eksempelet en slags følelse av hva slags eventyr som interaktive romaner kan romme?

Det er langt fra disse tidligere eksemplene til dagens spill. Jeg tror vi er kommet over den tiden da datamaskinbaserte spill først og fremst ble assosiert med slagsmål og kappløp med raske bilder. Hvor spillerens oppgave var å eliminere så mange motstandere som mulig med våpen eller fantasifulle slag og spark, samtidig som spilleren selv skulle unngå å bli drept. Dette var spill som bokstavelig talt var basert på en korridor-modell: Spilleren startet i den ene enden av korridoren, og slo seg så fremover mot mål.

Men det kan likevel være med på å eksemplifisere at spill har en dramaturgi. Korridor-modellen er enkel: Spillerens oppgave er å bevege seg i korridorens retning, riktignok kan det være omveier gjennom sidegrener, men stort sett er det rett frem. Samtidig blir korridoren en tidslinje som spillet utvikler seg langs, det minner litt om en film. Spillerens kontroll er redusert til å løse oppgavene langs veien. Og det kan være spennende nok.

Men Trinity gir et eksempel på en litt annen modell, forum-modellen. Spilleren plasseres i en situasjon og får så selv velge hva som er neste skritt. Det blir som å stå på et torg med boder – så lenge man bare står det, skjer nesten ingen ting. Men må selv ta det første skrittet inn i en bod, snakke med dem man finner der, se hva som måtte skjule seg der inne. Her har ikke spillmakeren samme lineære kontroll. For å illustrere det: La oss tenke oss at det er en mordgåte, og at det avgjørende beviset er et brev fra den avdøde. Det ville være kjedelig om spilleren bestemte seg for å gå inn i biblioteket, åpne skrivebordet, finne brevet og avslutte spillet i tre trekk. Spillmakeren må sørge for at hvis spilleren begynner slik, så mangler brevet i skrivebordskuffen: Spilleren hindres av spillets logikk å lese den siste siden først, det avgjørende skrittet kan først tas når andre og nødvendige skritt er tilbakelagt. Det er betydelig mer utfordrende å lage et spill etter forum-modellen enn etter korridor-modellen.[3]

3 Selv har jeg faktisk forsøkt å lage et spill etter forum-modellen, jfr *Savnet i Lokaya – Human Quest I*, Universitetsforlaget og Norges Røde Kors, Oslo 1996 – jeg bidro bare med et første utkast.

Og dette er bare en antydning av de dramaturgiske utfordringene og mulighetene i spillene. Et annet viktig element er at spillene ikke bare befolkes av de personer og vesener som spillmakeren har utformet. Spillene tillater at spilleren selv trer inn i spillets virkelighet. Spilleren velger seg en avatar – et uttrykk som er lånt fra sanskrit Avatāra, som betyr «inkarnasjon», og opprinnelig refererte til hvordan et guddommelig vesen viste seg i vår verden. Spilleren kan velge fra et galleri av avatarer, men spillet kan også la spilleren utforme sin egen avtatar. Slik fremstår spilleren som en del av spillet, han eller hun er synlig for de andre spillerne. Og spillet tillater selvsagt også at avtaren har en viss frihet til å gjøre valg, til å kommunisere med andre avtarer og – selvsagt – utfordre dem til kamp.

Det kan være mange spillere samtidig tilstede i disse spillverdenene. I «massive direktekoblede multispiller rollespill»[4] er kompleksiteten svært høy. Avatarene blir dyktigere etter hvert som spillerne lærer om mulighetene. Hjelpemidler kan konstrueres. Et sverd som brukes flittig, lar avtataren oftere seire i dueller.

Eksempelet antyder at dette beslektet med rollespill som Dungeons and Dragons,[5] hvor spilleren inviteres inn i et fantasiland med drager, trollmenn og andre eventyrskikkelser – ofte omgivelser som minner om de JRR Tolkien har gjort berømte i sin trilogi om Ringenes herre.[6] Noen av de mest populære spillene tilhører nettopp denne kategorien, som f eks World of Warcraft. Denne fantasiverdenen ble først introdusert av Blizzard Entertainment i 1994 (Warcraft: Orcs & Humans), og senere er nye utgaver kommet. Det anses for å være verdens mest populære i sitt slag, med ca 8 millioner abonnenter[7] over hele verden. Det vil altså si at det «bor» omtrent dobbelt så mange mennesker i denne liksomverdenen enn i Norge. Til enhver tid er det hundretusener av spillere koblet til spillet, som danner forbund og legger planer for å mestre ny utfordringer.

Men omgivelsene kan være ganske annerledes alminnelige. Et eksempel er Second Life, en tredimensjonal verden som ble lansert av Linden Labs i 2003. Dette er nærmest en datamaskinbasert kopi av hverdagens verden. Her har IBM kontorer, Sony butikker – valutaen er konvertibel, og man kan f eks kjøpe seg en tomt og bygge et hus (da må man selvsagt kjøpe materialer og finne de nødvendige ressursene for å konstruere det). Og så kan man forsøke å selge eiendommen til andre «innbyggere». Ailin Graef ble nylig den første millionæren på denne måten. Avataren hennes kjøpte billig virtuelle tomter,

4 MMORPG («massively multiplayer online role-playing games»).
5 *D&D* var opprinnelig et rollespill støttet av et brettspill, utviklet av E Gary Gyax og Dave Arneson, først utgitt i 1974.
6 *The Lord of the Rings*, 1954-55.
7 August 2007.

utviklet dem, delte dem opp og hun solgte dem med fortjeneste i virkelighetens verden.[8] Riktig så stort som WoW er ikke dette spillet, men det har mer enn fem millioner brukerkonti.

Med slike brukertall kan man liksom ikke skyve spillene til side. De er viktige deler av moderne kultur, på linje med musikk, drama og film. De har da også etter hvert fått oppmerksomhet, nye spill bli anmeldt og vurdert. Dramaturgi og pedagogikk i spillene er komplekse og sofistikerte. Virkemidler kan vurderes i flere perspektiv – kunstnerisk, teknisk, forretningsmessig. Opplevelsene er svært forskjellige.

Disse perspektivene i spillene kan jeg bare så vidt antyde, og på ingen måte yte rettferdighet. Mitt poeng er litt forskjellig. Spill – som f eks Second Life – kan også oppfattes som et grensesnitt mot Nettet.

Noen av oss husker da grensesnittet var tegnbasert. En kommandolinje med grønne eller gule tegn mot en svart skjerm, eller hvite tegn mot blå bakgrunn. Slik var grensesnittet for Trinity, det fungerte for interaktive romaner. Men heldigvis har vi nesten glemt dette. Apple introduserte et grafisk grensesnitt for sin Macintosh i 1984, etter hvert fikk også andre operativsystem grafisk grensesnitt. World Wide Web ble utviklet i 1990, den første nettleseren – Mosaic – kom i mars 1993. Og da fikk også Nettet et grafisk grensesnitt.

Det er nettopp det grafiske grensesnittet til World Wide Web og nettlesere de fleste av oss kjenner og daglig bruker. Et øyeblikk kan vi kanskje tenke etter hvor forskjellig skjermbildet er fra de boksidene vi vokste opp med: Ikke bare er det forskjeller i variert typografi, grafikk med farger og bevegelser – det er også hyperlenker og søkemuligheter som får fotnoter eller bak-i-boken registre til å virke nokså puslete. Også dette er et nytt medium, og forstås av brukere helt forskjellig fra en bokside.

Men likevel er mange begrensninger velkjente. Skal vi kommunisere, sender vi et e-brev, ikonet er ofte et lite bilde av en konvolutt med et frimerke, som om dette skulle forklare hva som skjer – det er i virkeligheten en referanse til en fordums virkelighet, som om vi skulle forklare et fjernsyn med å vise et lite bilde av en teaterscene. Vi kommuniserer også med lyn- og tekstmeldinger. Bruken av et lite kamera for toveis billedkommunikasjon har ikke helt slått gjennom.

Poenget er at vi bruker separate tjenester. Vi sender et brev, vi søker i Google, vi slår opp i en nettavis. I Second Life henger alt sammen på en annen måte. Vi er selv til stede som en avatar i den virtuelle virkeligheten som Nettet representerer. Det er som om vi har sendt en agent inn i verdenen bak skjermen. Den virtuelle virkeligheten er noe mer enn tekst, grafikk og lyd – den er

8 Anna Raciti «Fantasiens rikdom», Lov&Data 91/2007:22-24.

blitt sammenhengende, kontinuerlig og oppleves av vår avatar. William Gibson fant opp ordet «cyberspace» for å beskrive dette.[9]

Og jeg tenker tilbake til min barndoms bordplater med plastelinafigurer. Modellverdenen på platene var på en måte en slags fattigmannsversjon av World of Warcraft eller Second Life. Jeg husker beruselsens fra leken i skogen ved vannet om somrene – hva om jeg kunne ha tatt med meg den hjem, ikke bare landskapet med fantasiens ville dyr og svikefulle blekansikter, men også vennene mine – de jeg ellers bare møtte om sommeren. Vi kunne slått oss sammen, jeg som avtataren Silver Horse, og som i følge med muntre kamerater utfordret farene i liksomverdenen bak skjermen.

Men det er likevel bare en begynnelse.

Tenk deg et mulig sluttbrukerutstyr. Først høyttalerne, en for hvert øre, full stereolyd. En mikrofon limt på kinnet. Glem skjermen. Tenk i stedet på en forbedret utgave av Virtual Retina Display,[10] utviklet ved Univrsity of Washington Human Interface Technology Lab 1991. Lasestråler projiseres direkte gjennom pupillene på netthinnen og danner høyoppløselige fargebilder som dekker hele synsfeltet. Venstre og høyre bilde er litt forskjellig, en forskjell som av hjernen tolkes som tre dimensjoner: Man ser ikke et bilde på en skjerm, man ser inn i et tredimensjonalt rom.

Glem tastaturet. Tenk i stedet på en forbedret datahanske. Slike finnes i virkeligheten, «Data Glove» er for eksempel et varemerke for Sun Microsystems. Følere registrerer bevegelser til fingrene. Haptisk tilbakebobling lar deg oppleve berøring. Forbedrede utgaver vil kunne ha hydraulisk styrte nupper innvending som imiterer enhver tekstur – fra myk hud til grov grus. Mikroklima lar deg føle om det er varmt og fuktig eller kaldt og tørt. Hansken kan stivne i enhver stilling, og gi illusjonen av at du stryker noen over kinnet eller griper om et jernrør.

Med stemmen kan du gi kommandoer. Vi forutsetter ikke at stemmegjenkjenning eller forståelse av naturlig språk er kommet stort lenger enn i dag. Men allerede kan vi gi kommandoer som styrer systemer: «Ring hjem!», «På med lys!» og så videre. Noe tastatur har vi ikke. Det har heller ikke en berøringsskjerm. Si: «Vis tastatur!», så dukker det et tastatur opp i vårt tredimensjonale synsfelt, som vi kan skrive på med våre hanskekledde hender. Hvis vi skulle trenge det. For det er nok av andre ting vi kan gjøre i den virtuelle

9 I romanen Neuromancer (1984), som han faktisk presenterte ved sin atavar på et foredrag i Second Life august 2007. Boken er oversatt av Torgrim Eggen, til norsk som Nevromantiker (Aschehoug , Oslo 1999).

10 Se http://www.cs.nps.navy.mil/people/faculty/capps/4473/projects/fiambolis/vrd/vrd_full.html.

verdenen uten tastatur. I vår vanlige hverdag klarer vi jo oss godt uten. Vi kan åpne en dør, vinke til en venn, klappe en katt …

Forresten har hanskene vokst. De er blitt til en tettsittende kroppsdrakt med innvendige nupper hele veien rundt, direkte i kontakt med naken hud. Nå kan du føle varmen av solen i ansiktet, spruten fra bølgene langs stranden, de skarpe klørne til katten som maler i armene dine. Og du kan flytte deg i landskapet ved ganske enkelt å gå, eller late som du går. Kanskje hoppe på et virtuell trikk for å komme fortere frem. Eller kjøre en virtuell bil …

Kanskje det også er små sonder som fører til munn og nese, og som blander bittert og søtt, syrlig og salt og lar deg smake på et eple eller kjenne duften av nybakte vafler?

Dette er en skisse av fremtidens grensesnitt. Det finnes ikke i dag. Men de fleste komponentene finnes. De er bare ikke satt sammen til forbrukerelektronikk.

Men tenk deg at du hadde en slik kroppsdrakt med trådløs bredbåndstilknytning til Nettet. Tenk deg da at du trådte inn i World of Warcraft. Du dukker opp i skikkelsen til din atavar, håndhilser på de av dine kamerater som akkurat nå er logget inn. Tar deg tid til litt småprat, ser deg om – den susende furuskogen som lukter friskt, vannet som glitrer nedenfor bakken. Du veier spydet i hånden, skygge for solen med det sølvblanke skjoldet med omrisset av en hest …

Mulighetene er like mange som fantasien tillater. Med andre ord ubegrensede.

Gjennom speilet og hva Alice fant der[11] er tittelen på den andre fortellingen om Alice av Lewis Carroll. Eventyrene ga speilet omtrent samme funksjon om en skjerm, det reflekterte ikke bare ansiktet til den som så i det, speilet kunne også brukes til kommunikasjon og gi svar på spørsmål – hvem husker vel ikke den onde dronningens spørsmål til sitt magiske speil: «Hvem er vakrest i landet her?»

Og Lewis Carroll røpet i sin andre fortelling om Alice hvordan klatret opp på kaminhyllen, og hvordan speilet liksom smeltet til en tåke av sølv, og hun plutselig var på den andre siden, i den speilvendte verden, nesten lik vår egen, men likevel «så forskjellig som det går an» – et «second life».

Det ville være fåfengt å forsøke med en oppregning av hva en slik teknologi kan brukes til. Man kan tenke seg at man har sett den første flimrende filmen av svarte og hvite bilder i begynnelsen av det 20. århundre, og så forsøker å forklare det nye mediets potensial – ikke bare som eventyr og kunst, men som dokumentasjon, reportasje og undervisning. Men det er åpenbart at potensialet

11 Through the Looking-glass and what Alice found there (1871).

til den virtuelle virkelighetsteknologien er enda større for drama, romantikk og pedagogikk. Man kan ikke bare parallellforskyve filmens muligheter, den store forskjellen blir at til filmen er man tilskuer, mens man i den virtuelle virkelighet er deltaker gjennom sin tilstedeværende avatar. Ikke bare vil andre spilleres avatarer kunne trenge seg inn i handlingen, spillmakerens figurer styres av autonome datamaskinprogrammer og vil å samhandle med avtatarene. Og naturligvis alle de andre mulighetene – din avtatar er menig soldat i Vietnams jungel, din avtatar er en smart rakettbombe på vei mot en bunker i Irak, din avatar står ved siden av kirurgen og rekker ham skalpellen idet han skal gjøre det første snittet for å blottlegge et feilfungerende hjerte …

Som sagt, det er fåfengt å oppregne mulighetene. Men det er lett å tenke seg at «virkelighetsflukt» får et nytt innhold.

«De evige gleders palass» forekommer i en fortelling av Will Worthington.[12] Palasset minner om en drueklase, hver drue er fylt av en næringsvæske som det flyter mennesker i, knyttet til kybernetiske systemer av slanger og kabler. Rundt palasset er byen falt i ruiner, men menneskene drømmer videre hjulpet av maskiner som får energi fra solstrålene. Det er en ekkel, forførende visjon. Og varsler hvordan mange vil reagere på den virtuelle verdensteknologien. Vi vil advare mot den, frykte de nye opplevelsene – på samme måte som vi tidligere reagerte på film. På tegneserier. På fjernsyn. På interaktive spill. På selve Nettet.

I 1972 landet Apollo 17 på Månen. I dag er det over tredve år siden et menneske satte fot på en annen klode. Men 1972 var også året da de rutinene som gjorde elektronisk post mulig, ble integrert i det rudimentære Internettet.[13] På en måte kan man si at mens reisen til det ytre rom ble avviklet, konstruerte man de verktøy som skulle gjøre det mulig å reise i det indre rom – det univers av kunnskap, innsikt, drømmer og fantasier som mennesker selv har skapt. Et univers som er like ubegrenset, og like raskt ekspanderende, som selve verdensrommet.

12 Will Worthington «Plentitude» (1960), gjengitt som «Det søte liv» i Bing & Bringsværd Tider skal komme, Gyldendal, Oslo 1968:169-178.

13 Programmene SNDMSG og READMAIL, utviklet av Ray Tomlinson, MIT.

«I STRAFFERETTSPLEIENS TJENESTE»

NOEN MILEPÆLER I HISTORIEN OM REGISTRERING OG BRUK AV OPPLYSNINGER OM STRAFF

Herbjørn Andresen

Innledning

Strafferegisteret inneholder opplysninger om dommer og avgjørelser om straff. De typene straff det dreier seg om er listet opp i strafferegistreringsloven[1] § 1. Opplysningene i Strafferegisteret kan brukes i ny etterforskning og rettsforfølgelse mot en tidligere straffet person, slik det følger av ordlyden i strafferegistreringslovens § 2 første ledd: «Til bruk for strafferettspleien kan politiet, påtalemyndigheten og domstolene begjære straffattest med opplysning om avgjørelser som er ført inn i Strafferegistret.»

Dette nøkterne og greie utgangspunktet, i en mer enn 35 år gammel lov, befinner seg i et historisk veikryss. Norges første sentrale strafferegister ble påbegynt i 1902, med opplysninger tilbakedatert til 1. januar 1901. Frem til strafferegistreringsloven trådte i kraft var adgangen til å gjenbruke opplysninger fra Strafferegisteret ved senere etterforskning eller sak mot samme gjerningsperson hjemlet i en kongelig resolusjon. Da strafferegistreringsloven ble vedtatt i 1971, var en omlegging av Strafferegisteret til EDB allerede utredet men ennå ikke iverksatt.

De rettslige, teknologiske, organisatoriske og kriminalpolitiske omgivelsene som strafferegistreringsloven fungerer under har vært og er i rask utvikling. Utviklingen omfatter blant annet økt etterspørsel etter opplysninger, og fremveksten av generelle regler om behandling av personopplysninger, først i personregisterloven[2] og senere personopplysningsloven[3]. Det handler også om harmonisering av begrepene som brukes i strafferettspleiens ulike institusjoner, og teknologisk interoperabilitet[4] mellom strafferettspleiens IT-systemer.

---

1 Lov om strafferegistrering, 11. juni 1971 nr. 52
2 Lov av 9. juni 1978 nr. 48 (opphevet)
3 Lov av 14. april 2000 nr. 31
4 Betegner egenskaper og tiltak som gjør det mulig å oppnå samhandling mellom to eller flere IT-systemer

Arbeidet med en ny politiregisterlov har pågått lenge[5], men er ennå ikke i mål. Politiregisterloven er ment å erstatte strafferegistreringsloven, samtidig som den er bedre tilpasset både til integrert informasjonsbehandling i straffesakskjeden og til nyere generell persondatalovgivning.

Denne artikkelen presenterer noen historiske milepæler i strafferegistreringen. Mange av milepælene dreier seg om mulighetene for å gjenbruke opplysningene etter at en straff er registrert, og sonet eller gjort opp. Samtidig som dette er en historie om store teknologiske og faktiske endringer, er det også en historie om nærmest forbausende stabile problembeskrivelser og ambisjoner.

Det franske forbildet, Casier judiciaire

Forbildet for det norske Strafferegisteret var det franske systemet *Casier judiciaire*, som ble opprettet ved et ministerielt sirkulære av 6. november 1850. Registeret var basert på løse kort som ble plassert i åpne esker uten lokk. Forslaget om et slikt register ble fremmet to år tidligere av en av pionerene innen kriminologi, Arnould Bonneville de Marsangy[6].

Bonneville forsket på effektene av straff og fangebehandling, og tok også initiativet til omfattende reformer. Han var opptatt av, og er kjent for å ha satt på den kriminalpolitiske agendaen, komplementære virkemidler i utkanten av den ordinære strafferettspleien. Virkemidlene omfatter blant annet erstatning til ofre, benådning, prøveløslatelse, ettervern og rehabilitering. Disse ideene ble utdypet i hans bok «*Traité des Diverses Institutions Complementaires de Régime Pénitentiaire*»[7] (1847). Et av de problemene som opptok Bonneville var forbryteres tilbakefall til nye straffbare handlinger. Siden tidlig på 1800-tallet definerte fransk lovgivning høyere maksimumsstraffer for gjengangerkriminelle[8]. At man var tidligere straffet kunne også være bestemmende for hvilken type straff, og hvilke sikkerhetstiltak under soning, som ble iverksatt. Derfor var det nødvendig å vite om den tiltalte i en sak hadde vært dømt tidligere.

---

5 Utredning levert 28. august 2003, NOU 2003:21, Kriminalitetsbekjempelse og personvern – politiets og påtalemyndighetens behandling av opplysninger. Høringsfrist for utredningen var 1. april 2004

6 Omtalen av Bonneville og etableringen av straffekartoteket «Casier Judiciaire» er basert på André Normandeaus artikkel «Pioneers in Criminology: Arnould Bonneville de Marsangy (1802-1894)», i The Journal of Criminal Law, Criminology and Police Science 1969, vol. 60 nr. 1, s. 28-32.

7 Som amatør i det franske språk oversetter jeg denne boktittelen til «Utredning om de ulike institusjoner som er komplementære til straffesystemet»

8 Forhøyet straff ved gjentakelser har også lang historie i norsk lovgivning, tilbake til Magnus Lagabøtes landslov på 1200-tallet. Særlig innebar gjentatte tyverier en nokså kraftig progresjon i den angitte maksimumsstraffen

Dette var bakgrunnen for Bonnevilles idé om å opparbeide en pålitelig og komplett fortegnelse over alle tidligere dommer mot samme gjerningsmann. Forslaget ble utformet i et memorandum med den nærmest heldekkende tittelen *«De la localisation au Greffe de l'Arrondissement Natal des Renseignements Judiciaires Concernant Chaque Condamné: Les Casiers Juciciaires»*[9] (5. november 1848). Det foreslåtte systemet ville skape et alfabetisk ordnet kartotek ved hver distriktsdomstol, som inneholdt dommer mot personer født i dette distriktet, uavhengig av når og hvor dommen var avsagt.

Casier judiciaire ble etablert i Frankrike i 1850. I følge Normandeaus artikkel om Bonneville ble det franske systemet senere kopiert i de fleste europeiske land, og man begynte relativt tidlig å utveksle informasjon mellom landene.

Forslag om et strafferegister i Norge

Assessor Anders Færden[10] i Kristiania byrett var en tidlig pådriver for å få opprettet et systematisk strafferegister i Norge. Under et studieopphold i Paris i 1895 studerte han det franske systemet, og gikk sterkt inn for å innføre tilsvarende system under felles regelverk og med en viss grad av felles registerføring mellom de nordiske landene[11].

I 1899 utga Færden en artikkel[12], med tittelen *Om Fællesskab eller ensartethet med hensyn til bestemmelser om strafferegistre i de nordiske lande.* Artikkelen var utgitt som forhandlingsemne ved niende nordiske juristmøte i Kristiania samme år[13]. Færdens artikkel beskrev behovet for et systematisk strafferegister, redegjorde for liknende registre i andre europeiske land og da spesielt inngående for de øvrige nordiske land, og presenterte begrunnede forslag om registerets innretning.

---

9 Mitt forsøk på å oversette tittelen fra fransk lyder slik: «Om lokalisering på kontoret til det domstolsdistrikt der vedkommende er født, av informasjon om rettsavgjørelser angående hver enkelt domfelt: Straffekartoteket.»

10 Anders Færden (1860-1939) var dommer og byrettsjustitiarius i Kristiania/Oslo byrett 1898-1930. Han utga også en rekke bøker om ulike juridiske emner

11 Norden omfattet den gang de tre landene Danmark, Sverige og Norge (som var i union med Sverige). Island ble delvis selvstendig fra Danmark i 1918, og helt uavhengig i 1944. Finland ble selvstendig fra Russland i 1917.

12 Artikkelen ble trykket som egen bok (13 sider, 36 sider inkludert vedlegg). Aktie-bogtrykkeriet, Kristiania 1899. Sitatene i det følgende avsnittet om Færdens forslag er hentet fra nevnte artikkel

13 **Det nordiske juristmøtet 1899 hadde et tett program, og den oppsatte tiden strakk ikke til.** Derfor ble tre av emnene, deriblant Færdens, utsatt til neste nordiske juristmøte i København 1902. En revidert utgave av artikkelen fra 1899 ble gitt ut som forhandlingsemne til juristmøtet i 1902.

Behovsbeskrivelsen, og vurderingene av hvordan et register bør innrettes, må sies å være fremsynte. Flere grunnleggende elementer i drøftingen fra 1899 har vært relevante ved ulike senere milepæler i strafferegistreringen. De samme elementene er fremdeles relevante i den nåtidige omfattende informasjonsintegrasjonen som er under planlegging og gjennomføring i justissektoren.

Færdens begrunnelser for behovet for et strafferegister

I begynnelsen av Færdens artikkel angir han fire grunnleggende formål med strafferegistrering. Selv om han ikke lister opp disse formålene i klart avgrensete punkter, kan fire hovedpunkter nærmest hentes direkte ut av hans egne formuleringer – som er sitert i en parentes under hvert punkt:

- Kunnskap om tidligere straff
  (Spørgsmålet om forhøiet Straf i Gjentagelsestilfælde.)
- Kontroll med soningen, og kunnskap om eventuelle særskilte tiltak under soning
  (Betydning for den under Fuldbyrdelse af Frihedsstraf særlig i vor Tid saa sterkt fremtrædende individuelle Behandling for at paavirke vedkommende moralsk.)
- Vandelsattester
  (At kunne bringe paa det rene, hvorvidt en Person har begaaet nogen Handling som formindsker hans «Æresret» eller gjør Skaar i hans Krav paa Medborgeres Agtelse og Tillid, saaledes ved Spørgsmaal om Stemmeret i Stat eller Kommune, om Adgang til aa opnaa forskjellige Næringsbevillinger, Haandverks- og Handelsborgerskab m. v.)
- Statistikk
  (Hensynet til Kriminal- og Socialstatistiken, hvis Opgaver danner en meget væsentlig Rettesnor ved Bedømmelsen af den gjældende Straffelovgivnings Virkemaade og Afgjørelsen af, om den i noget Stykke bør forandres.)

Det første av disse fire formålene, kunnskap om gjerningspersonens tidligere dommer, er det tyngst vektlagte argumentet i Færdens artikkel. Det skyldes nok først og fremst foredragets målgruppe, som er nordiske jurister. Samarbeid mellom landene om registrenes innretning er nødvendig fordi en del kriminelle opererer på tvers av landegrensene:

> *De bekvemme og hurtige Samfærdselsveie og Midler, de indbyrdes nærstaaende Sprog og Seder gjør det i vore Dage meget let at forlægge sin*

> *Forbrydervirksomhed fra Sverige eller Danmark til Norge eller omvendt, naar Myndighederne i det ene Land bliver vedkommende for ubehagelige og nærgaaende.*

Dernest ser det også ut til at problemet med kunnskap om tidligere dommer er det som er vanskeligst å få løst gjennom de daværende eksisterende informasjonskanaler:

> *Til Erhvervelse af de fornødne Oplysninger særlig under Strafforfølgningens sager angaaende den sigtedes (tiltaltes) mulig tidligere begaaede Lovovertrædelser har man fra først af vistnok overalt maattet holde sig til, hvad vedkommende selv godvillig oplyste, og til Berigtigelse har man alene havt mere eller mindre tilfældige Kundskabskilder, saasom vedkommende Politimænds eller andres Erindring om den sigtedes (tiltales) tidligere Straffældelser og desl. Dette system, som egentlig intet er, kan man, for at tage et Navn, kalde «Bonafide-Systemet».*

Færden nevner også det norske *Polititidende*, som sammen med de svenske *Polisunderrättelser* og de danske *Politiefterretninger* kan gi verdifull kunnskap om tidligere straffede personers vandel, men:

> *Mangelen af fortløbende Registre og Opstillingen af de meddelte Oplysninger gjør det noksaa vanskeligt at benytte disse Publikationers Opgaver udenfor den nærmeste Tid efter Udgivelsen.*

De eksisterende informasjonssystemene var altså utilstrekkelige for alle de fire nevnte formålene, og da i særdeleshet utilstrekkelige for å gjenfinne opplysninger om gjerningspersonens tidligere straffbare handlinger.

Utbredelsen av tilsvarende strafferegistre i Europa

Assessor Færdens forslag om strafferegister representerte ikke i og for seg noen ny eller ukjent tanke:

> *Det bemerkes, at den internationale Fængselskongres i Rom i 1885 og den internationale Kriminalistforening paa sin Konference i Antwerpen i 1894 har anbefalet alle Stater at indføre et lignende Strafferegistersystem som det ovenfor beskrevne franske.*

De land som har innført et slikt system pr. 1899 er «Portugal, Italien, det tyske Rige, Belgien, Holland, et Par Schweitzer-kantoner og Ungarn». Danmark hadde ved et sirkulære fra Justisministeriet 11. desember 1896 innført et protokollbasert strafferegister, som føres ved den domfeltes fødejurisdiksjon. Den danske løsningen var altså delvis basert på den franske, ved at opplysninger om samme person ble samlet i samme register, men det var ikke innrettet som løse kartotekkort i åpne esker. I Sverige forelå det et lovforslag[14] om et sentralt register.

Organisering og innretning av strafferegisteret i Færdens forslag

I utgangspunktet nevnes tre forskjellige registersystemer som kan brukes til de formålene som er beskrevet: Protokollasjonssystemet, eskesystemet (samme som *Casier judiciaire*), og rullesystemet. Færden avviser protokollasjonssystemet som lite egnet. Det medfører atskillig arbeid med avskrifter, nødvendiggjør et særskilt navneregister, og gir ikke mulighet for sletting av overflødige opplysninger.

Eskesystemet fungerer «saa at man øieblikkelig har den paagjældende indført ved at stikke Kartonbladet ind paa sin Plads, og kan slippe at føre noget særskilt Navneregister». Systemet tillater også «Udskillelse af Blade vedkommende Personer, som er døde, eller hvis Domfældelser er bleven saa gamle, at de ikke længer har Interesse». Rullesystemet er permer med løse blader som kan settes inn og tas ut ved behov, tilsvarende det som «man i Norge benytter til Opbevaring af de militære Rulleblade». Rullesystemet har mange av de samme egenskapene som eskesystemet. Det er noe mer tungvint å holde à jour, men krever mindre plass enn esker med kartotekkort. Færden anser både eskesystemet og rullesystemet som egnet. Valg av registersystem og fysisk utforming er imidlertid ikke det viktigste elementet i drøftingen av registerets innretning.

Færden regnet det som sikkert at man ville få et strafferegistersystem i Norge, det var «utvivlsomt blot et Tidsspørgsmaal». Hensikten med forslagene var å peke på hva som skulle til for å lykkes, slik at registeret ble nyttig og effektivt. Blant de elementene han argumenterer for er:

14 Da artikkelen ble trykket, i 1899, forelå et svensk lovforslag fra 1892 som var trykket som vedlegg. Da Færden først slapp til med sitt innlegg, på det tiende nordiske juristmøte i 1902, var den svenske loven allerede vedtatt. Den ble vedtatt den 17. oktober 1900

- Straff bør registreres etter fødested, og ikke bosted. Fødestedet er mer stabilt, og «Ethvert System, som tillader Skiftning, er nemlig en Kilde til Feiltagelser»
- For å oppnå utstrakt bruk på tvers av nordiske land, bør regler for føring av registrene, registrenes utforming og tilhørende skjemaer være ensartede mellom landene
- Det burde også «tilveiebringes Overenskomster [...] med andre Stater i og udenfor Europa om direkte Udveksling af Meddelelser mellom Registrerin gsmyndighederne»
- Identifisering og autentisering av gjerningspersoner. Dette punktet vies lite plass i artikkelen, men det nevnes at både identifiserende opplysninger («mere betryggende Familiestandsregistere end de nu paabudte Ministerialbøger») og gjenkjenning («Anvendelse af det anthropometriske eller et andet betryggende Identifikationssystem») er nødvendig for å oppnå full nytte av strafferegistrene
- Regulering av hvem som kan få opplysninger om en person, når, og til hvilke formål, blant annet for å unngå misbruk av registeret

Færden nevner at det i noen land er gitt adgang til at vedkommende person selv kan få utdrag fra *Casier Judiciaire*. Det innebærer altså en form for innsynsrett for den registrerte. En slik innsynsrett er imidlertid ikke tatt med som en del av hans konkrete og begrunnede forslag til innretning av et norsk strafferegister.

Det er vanskelig å si noe sikkert om hvor stor innflytelse Færdens argumenter hadde ved etableringen av Strafferegisteret. Det som imidlertid er interessant med hans artikkel fra slutten av 1800-tallet, før Strafferegisteret ble etablert, er bredden og presisjonsnivået i drøftingen av faglige problemstillinger.

Fengselsstyrets sentrale strafferegister

Landets første sentrale strafferegister ble etablert ved en beslutning fra Fengselsstyret i april 1902, som gikk ut på at «direktørene for landsfengslene skulle sende inn til Styret særskilte tellekort som gav nærmere opplysninger om alle dem som var satt inn til utholdelse av frihetsstraff»[15]. Opplysningene i registeret skulle omfatte alle innsettelser i landsfengsel fra januar 1901.

Strafferegisteret besto av to typer kartotekkort, henholdsvis registerkort og tellekort. Registerkortene identifiserte personer, for hurtig å finne frem til

15 Jf. Innstilling fra Straffelovrådet om Lov om strafferegistrering, av mars 1967, s. 7

hvorvidt en person var registrert som straffet[16]. Tellekortene var mer detaljerte, og inneholdt også opplysninger om endringer underveis i en soning, for eksempel refs eller overføring til annen anstalt. Tellekortene var kartongkort som ble sendt inn fra anstaltene, mens registerkortene ble ført ved Fengselsstyret. Nytt registerkort ble fylt ut dersom registeret mottok et tellekort som gjaldt en ny person, som det ikke allerede fantes registerkort for. Over tid mottok registeret flere tellekort for hver registrert person.

Denne innrapporteringen og registreringen var Strafferegisterets spede begynnelse. Formålene med registreringen fra Fengselsstyrets side var å styrke kontrollen med straffefullbyrdelsen, og å føre statistikk over landsfengslenes virksomhet. Dette var i samsvar med to av de fire formålene som Færden hadde anført i sin artikkel. Fra begynnelsen av ble ikke registeret benyttet til å utstede vandelsattester, og det ble heller ikke brukt i etterforskning og straffeforfølgelse ved nye straffbare handlinger.

Veien frem mot å bruke Strafferegisteret ved nye saker mot tidligere straffet person

Tanken om at Strafferegisteret kunne være et nyttig verktøy for å skaffe kunnskap om en gjerningspersons tidligere straffer var sådd allerede før registeret ble etablert. Likevel kom ikke praksisen med å sjekke Strafferegisteret under etterforskning eller påtale uten videre på plass av seg selv. I mange år forble hovedprinsippet at man sjekket gamle rettsakter, i forsøket på å bringe på det rene om vedkommende var tidligere straffet. Man kan spekulere på om årsaken til tilbakeholdenheten med å bruke strafferegisteret til dette formålet var en sterk pietet for legalitetsprinsippet, at man følte behov for en klar hjemmel for slik bruk av registeret. En annen forklaring kan være at det snarere dreide seg om en langsommelig organisatorisk modningsprosess. Adgangen til, og praksisen med, å bruke straffekortene i nye saker vokste frem litt etter litt.

I 1909 åpnet Justisdepartementet for å ta i bruk straffekortene dersom man ikke fant fram i eldre rettsakter. En *Rundskrivelse fra Justisdepartementet* av 21. desember 1909 utdyper straffeprosesslovens krav til å kartlegge «angjældendes tidligere vandel». Rundskrivet innskjerper behovet for nøyaktighet, og stiller opp som hovedregel at man må «ha med de eldre akter ved sakens paadømmelse». Først mot slutten av rundskrivet, i punkt 7, åpnes det for bruk av Strafferegisteret:

16 Opplegget med registerkort for å raskt finne ut om en person var registrert eller ikke inngikk ikke i Færdens forslag. Tvert i mot anførte han behovet for et særskilt navneregister som et motargument mot protokollsystemet

> *Hvis ældre akter ikke kan findes efter de av sigtede meddelte oplysninger eller ved den fornødne undersøkelse i Polititidenden, vil der, ifald han har utholdt idømt fængselstraf (eller strafarbeide) eller været i tvangsarbeide, ved henvendelse til departementet, Fængselsstyrelsen, kunne erholdes et straffekort utvisende det tvangsarbeide og de idømte frihetsstraffe, hvis fuldbyrdelse er paabegyndt efter 1 januar 1901.* [17]

Det åpnes altså for at straffekortene tas i bruk når eldre rettsakter ikke kan oppdrives. Dette er således en subsidiær ordning, og det fremgår av senere utvikling at innhenting av straffekort neppe var veldig utbredt de nærmeste årene etter at dette rundskrivet kom. Byråsjef Hartvig Nissen[18] i Fengselsstyret hadde i mange år oppgaven med å utarbeide fangestatistikken. I «Tillæg til Fængselsstyrelsen Aarbok 1912», beskriver han noen metodiske problemer med å stille opp statistikk over tilbakefall til fengselsstraff. Koblingen mellom to saker mot samme person i statistikken var ikke basert på Strafferegisterets opplysninger, men på oppgaver utarbeidet på grunnlag av tidligere rettsakter. Han bemerker at «[…] akterne ofte var i en bedrøvelig forfatning».

Fengselsstyret og påtalemyndigheten er ulike etater i justissektoren. Det er Fengselsstyret som eier og driver Strafferegisteret, men det blir stadig klarere at registeret kan være til minst like stor nytte for påtalemyndigheten. En beslutning i Kongelig resolusjon 5. august 1921 markerte denne erkjennelsen. Resolusjonen innførte en ny § 63 i påtaleinstruksen fra året før. Hovedregelen ble nå at Fengselsstyrets strafferegister alltid skulle brukes for å kartlegge om en siktet var tidligere straffet.

> *Når siktelse reises, bør der av fengselsstyrelsens strafferegister erhverves utskrift, som skal inneholde fortegnelse over eldre dommer, som vedkommer siktede, med opplysning om disses datum, lovovertredelsens art, forøvelsestiden, straffen og dennes fullbyrdelse samt angjeldendes fulle navn, fødselsår og —dag og fødested.* [19]

I Fengselsstyrelsens årbok 1922, s. 2, er den ovennevnte resolusjonen omtalt:

---

17 Norsk Lovtidende 1909, annen avdeling, side 721

18 Hartvig Nissen (1874-1945) var byråsjef i Fængselsstyrelsen i Justisdepartementet i mange år. Blant arbeidsoppgavene var inspeksjon av fengsler og utarbeidelse av kriminalstatistikk. Han skrev en rekke artikler om ulike kriminalpolitiske emner. Fra 1924 var han direktør for Botsfengselet

19 Norsk Lovtidende 1921, annen avdeling, s. 412

> *Fengselsstyrelsen har siden 1901 hatt et strafferegister over fanger og tvangsarbeidere, i de senere år også over dem som har fått betinget dom m.v. Ved kgl. res. av 5 august 1921 blev det på foranledning av Justisdepartementet (dets Almindelige Avdeling) bestemt at dette register skulde tas i strafferettspleiens tjeneste i samme utstrekning som strafferegisteret i andre land. […] Etter forskjellige forberedende arbeider begynte den nye virksomhet 2 januar 1922.* [20]

I en faglig artikkel beskriver Nissen den nye ordningen med å bruke Strafferegisteret til å skaffe opplysninger om tidligere vandel, i stedet for å sende med de tidligere rettsakter. Fengselsstyrelsen («der som bekjendt er en avdeling av Justisdepartementet», skriver han) har ikke hatt noe å innvende mot den nye ordningen «naar Styrelsen bare fik den fornødne hjælp»[21].

Utvidelser i Strafferegisterets innhold

Det skjer også en omfattende innholdsmessig utvikling av Strafferegisteret gjennom dets første to tiår. Innrapporteringene kommer etter hvert fra flere kilder enn bare fra fengslene.

Nissen peker på en interessant, forvaltningsinformatisk årsakssammenheng: Innholdet i Strafferegistrert utvides over tid, og utvidelsene er klart og tydelig påvirket av utviklingen i hva registeret brukes til.

> *Som følge av sin utvidede opgave er strafferegistret blit øket med forskjellige indberetninger som det tidligere ikke mottok, særlig fra den militære strafferetspleie.* [22]

Registerets omfang utvides betydelig i perioden mellom 1901 og 1922, og utvidelsen foregår langs to akser. For det første øker omfanget ved at det er flere fengsler og anstalter som pålegges å sende inn tellekort. Da Staten overtok ansvaret for de lokale fengslene i 1904, traff Fengselsstyret tilsvarende vedtak

20 Dette avsnittet i Fengselsstyrelsens årbok fra 1922 bruker uttrykket «i strafferetsspleiens tjeneste» – som jeg også har valgt som tittel på denne artikkelen. Samme uttrykk ble brukt av straffelovrådet, da de i 1967 avga innstilling med forslag til strafferegistreringslov. Strengt tatt er dette en kuriositet, men likevel verdt å nevne: De pågående bestrebelser for å integrere informasjonsbehandlingen i straffesakskjeden er basert på teknologiske prinsipper som ofte omtales som «tjenesteorientert arkitektur». Måten begrepet «tjenester» brukes på i disse vidt forskjellige omgivelsene er i prinsippet den samme

21 Nordisk tidsskrift for strafferet, 1922 s. 136

22 Nordisk tidsskrift for strafferet, 1923, s. 179

om at også disse anstaltene skulle sende inn tellekort, på lik linje med landsfengslene som fikk dette pålegget i 1902. Fra 1915 ble de som var i arbeidshus i henhold til fattiglovene registrert, og fra 1922 ble også personer som sonet straff etter militær straffelov registrert i det sentrale Strafferegisteret. Den andre aksen er en utvidelse av hvilke typer straffer, dommer og beslutninger som registreres. De mest omfattende utvidelsene av hvilke typer beslutninger som skulle tas inn i registeret var:

- Fra 1. januar 1915: «Personer som har avsont straffen helt ut ved varetækt» og «personer som har faat betinget dom paa frihetsstraf»
- Fra 1. januar 1921: «Personer mot hvem paatale er undlat»
- Fra 1. januar 1922: «Personer som ved benaadning har faat fuldbyrdelsen av idømt frihetsstraf utsat […] eller helt eftergit eller faat idømt frihetsstraf omgjort til bøter»

Det var altså ikke lenger bare fengslene som var kilde til Strafferegisterets opplysninger, disse utvidelsene forutsatte at det også ble tilført opplysninger fra påtalemyndigheten. Innholdet i registeret utvides gradvis, og registreringen omfatter etter hvert et videre formål enn Fengselsstyrets egne informasjonsbehov.

Etter ett års erfaring med den nye ordningen i påtaleinstruksens § 63 skriver Nissen en liten oppsummering av erfaringene med bruk av Strafferegisteret for hele 1922. Det ble «rekvirert utskrifter vedkommende 2012 personer. Om 168 av dem hadde strafferegisteret ingen oplysninger at meddele, mens utskrift blev sendt for 1844 personer»[23]. Drøyt tjue år etter at strafferegisteret ble opprettet var altså påtalemyndigheten registerets største bruker, mens Fengselsstyret fremdeles var ansvarlig eier.

Politiets sentrale strafferegister

Kriminalpolitisentralen, Kripos, ble opprettet i 1959. I tiden fram til Politidirektoratet ble opprettet, i 2001, var Kripos direkte underlagt Justisdepartementet. I instruksen for Kripos, gitt i 1958, var sentral informasjonsinnsamling og formidling en viktig oppgave. Instruksen omfattet blant annet å føre register over personer.

Med bakgrunn i denne instruksen samlet Kripos inn ulike typer informasjon, både politifaglige opplysninger som kunne være av betydning for arbeidet med etterforskning og oppklaring av lovbrudd, og opplysninger om straffereaksjoner. Dermed vokste det fram et nytt sentralt register hos Kripos,

23 ibid.

som i stor grad inneholdt overlappende informasjon med Fengselsstyrets strafferegister.

Problemet med de to strafferegistrene

Innhenting av opplysninger fra Fengselsstyrets strafferegister hadde etter 1922 vært en helt alminnelig del av saksforberedelsen ved påtale. Man sendte en forespørsel, og tok seg tid til å vente på svar. Ordningen fungerte greit. Denne arbeidsformen egnet seg imidlertid ikke like godt for politiets bruk av opplysninger om tidligere straffedømte i etterforskningsarbeidet. For det første kunne politiet ha behov for tilgang til opplysninger utenfor Fengselsstyrets kontortid. For det andre hadde de ofte behov for å undersøke opplysninger om flere mulige mistenkte i en sak, som ledd i en etterforskning. En arbeidsform der man sendte enkeltforespørsler og ventet på svar var derfor lite effektiv. Kripos hadde etter hvert et enda større behov for tilgang til opplysninger om straffereaksjoner enn påtalemyndigheten, men det var vanskelig å få dekket behovet gjennom å bruke Fengselsstyrets register.

Problemet med at Strafferegisteret hadde ulike brukere med ulike behov ble løst på en ganske vanlig, men ikke særlig god måte. De som var pålagt å sende opplysninger inn til Strafferegisteret, først og fremst fengslene, ble pålagt å sende inn registreringskortene både til Fengselsstyret og til Kripos. Kortene til de ulike registrene hadde langt på vei samme innhold, men de var likevel ikke helt like. Størrelsen på kortene var ikke standardisert, bredden var litt mindre enn liggende A5-format (21 cm) i Fengselsstyrets register, og litt større enn liggende A5 i politiets register. Man kan således si at Justisdepartementet, som overordnet departement for begge registereierne, overså Færdens den gang omlag seksti år gamle anbefalinger om ensartethet. Frem mot 1970 hadde rapporteringspliktene blitt en belastning for fengslene, med unødvendig ekstraarbeid og sen saksgang[24].

Situasjonen med to parallelle strafferegistre var et sentralt spørsmål i forarbeidene til strafferegistreringsloven av 1971. Straffelovrådet, som avga innstilling med lovforslag i 1967[25], kom til den konklusjonen at registrene ikke burde

24 De konkrete problemene med ulike registerbrukeres behov, dobbeltarbeid og manglende standardisering er beskrevet i en rapport fra Politiets datagruppe. (Databehandlingsundersøkelsen i politiet: rapport, J. Johansson, A. Eskås og H. Svae, Oslo 1969). Politiets datagruppe utarbeidet noen få rapporter i perioden 1969-70, som både utredet mulighetene for å slå sammen strafferegistrene og ga anbefalinger om en gradvis omlegging til et EDB-basert strafferegister

25 Innstilling fra Straffelovrådet om Lov om strafferegistrering, av mars 1967. Straffelovrådet er et permanent sakkyndig råd for strafferettslige spørsmål, opprettet 1949. De begynte sitt arbeid med å utrede en strafferegistreringslov i 1955

slås sammen. Grunnene for å ikke slå registrene sammen var overveiende av prinsipiell karakter, de mente at de ulike etatenes oppgaver tilsa at registrene ble holdt atskilt. Høringsrunden viste at det var sterkt delte meninger om dette. Blant annet så riksadvokat Dorenfeldt det som «en vesentlig svakhet ved lovutkastet at det bygget på en forutsetning om at så vel Fengselsstyret som Kriminalpolitisentralen fortsatt skal føre hvert sitt register for hele landet»[26].

Spørsmålet om hvorvidt man skulle opprettholde to separate strafferegistre, eller om strafferegistreringsloven skulle holdes åpen for å kunne slå sammen registrene, var en av årsakene til at det tok lang tid før loven ble vedtatt. Detter er beskrevet i en artikkel i Lov og rett i 1970, året før strafferegistreringsloven ble vedtatt.

> *Forslaget fra politiets datagruppe var for øvrig en av årsakene til at lovforslaget om strafferegistrering ble stanset inntil videre. Forslaget ville bl.a. ha lovfestet en dobbeltregistrering, mens et av hovedprinsippene ved oppbygning av de elektroniske informasjonssystemene er at man skal unngå alle doble og flerdoble registreringer.* [27]

Justisdepartementet endret Straffelovrådets innstilling, slik at strafferegistreringsloven åpnet for at ulike aktører i strafferettspleien kunne bruke samme register. Adgangen til å bruke opplysningene fra Strafferegisteret ble, med den nye loven, mindre tett knyttet til etatsgrensene og eieransvaret for registeret. Det var også et uttalt mål fra departementets side at den nye loven ikke skulle stå i veien for omlegging til EDB:

> *Loven er så elastisk formulert at den ikke vil hindre at man går over til en sentralisert føring av alle registre etter moderne databehandlingsmetoder (fortrinnsvis EDB), dersom dette skulle vise seg hensiktsmessig i fremtiden.*[28]

Lov om strafferegistrering av 11. juni 1971 nr. 52 trådte i kraft 1. januar 1975.

---

26 Ot. prp. nr. 21 (1970–71), s. 20

27 Jon Bing, Elektronisk databehandling i rettsvitenskapen, Lov og rett 1970 s. 369 (sitert fra s. 376)

28 Ot. prp. nr. 21 (1970–71), s. 3

De to registrene slås sammen, og politiet overtar eieransvaret for Strafferegisteret

Politiets datagruppes rapport om databehandlingsarbeidet ved Strafferegisteret[29] foreslo å flytte strafferegistreringen fra Fengselsstyret til Kripos, og samordne dette med øvrige registreringsoppgaver der. I samme rapport ble det også foreslått å innføre edb-registrering. Mens Straffelovrådet førte en prinsipiell diskusjon om at registreringsoppgaver bør ses i sammenheng med et organs kompetanse, er det de praktiske hensynene som er vektlagt i rapporten. En av grunnene Politiets datagruppe anfører for at Kripos bør føre det nye felles registeret, er at de trenger døgnkontinuerlig tilgang til informasjonen. Fengselsstyrets register er bare tilgjengelig i kontortiden. En annen grunn til å legge registeret under Kripos er at det er et større informasjonsbehov der enn i Fengselsstyret. Dette er godt underbygget med statistikk over antall utskrifter fra registeret.

Selv om rapporten så vidt nevner at et av bruksområdene for Strafferegisteret er å dokumentere detaljer om fanger i forbindelse med Fengselsstyrets saksbehandling[30], går den ikke nærmere inn i en diskusjon om hvorvidt flytting av registeret til Kripos vil innebære noen svekkelse av Fengselsstyrets muligheter for å få dekket sine egne informasjonsbehov.

Fra 5. desember 1975 ble Strafferegisteret overført fra Fengselsstyret til Justisdepartementets politiavdeling. Hovedårsaken var en beslutning om å innføre EDB for behandling av straffe- og politiopplysninger.

> *Etter utløpet av denne beretningsperiode ble det i august 1975 holdt et møte i departementet om innføring av EDB-system for behandling av straffe- og politiopplysninger. Det var samtidig forutsetningen at den daglige ledelse av strafferegisteret skulle overføres fra Fengselsstyret til Justisdepartementets Politiavdeling. Slik overføring skjedde fra 5. desember 1975.* [31]

Kripos startet arbeidet med å innføre EDB-registrering omtrent samtidig med at de overtok ansvaret for Strafferegisteret. Hovedregisteret ble imidlertid fortsatt ført manuelt som kartotek frem til Det Sentrale Straffe- og Politiopplysningsregi ster (SSP) ble satt i drift ved Kripos 13. april 1982[32]. SSP er delt i to enheter. Stra fferegistreringsdelen inneholder ilagte straffereaksjoner, og har rettslig grunnlag

29 Databehandlingsundersøkelsen i politiet: rapport, J. Johansson, A. Eskås og H. Svae, Oslo 1969
30 ibid., s. 23
31 Fengselsstyrets årbok 1970–1974, s. 8
32 NOU 2003:21, s. 73

i strafferegistreringsloven § 1. Politiopplysningsdelen inneholder opplysninger som kan være av betydning for etterforsking og oppklaring av lovbrudd, og har hjemmel i strafferegistreringsloven § 4.

Den integrerte straffesakskjeden

Begrepet «strafferettskjeden» er brukt i kriminalmeldingen[33] fra 1992. I en sammenligning med den forutgående kriminalmeldingen, fra 1978, er 1992-meldingen kritisert for å legge uforholdsmessig stor vekt på administrasjon og effektivitet i de ulike involverte etatene[34]. Omtalen av strafferettskjeden i meldingens kapittel 2.3 må kunne sies å bekrefte oppfatningen om at det er stort fokus på hvordan ulike administrative problemer skal løses. Begrepet «strafferettskjede» introduseres med følgende definisjon:

> *Det apparat som samfunnet har etabler for å bekjempe kriminaliteten, kalles gjerne strafferettspleien eller straffesystemet. Strafferettskjeden er et begrep vi bruker for å betone det nære avhengighetsforholdet og det store samordningsbehov det er mellom de ulike ledd i behandlingen av lovbrudd og lovbrytere. De ledd eller institusjoner vi i første rekke tenker på, er politiet og påtalemyndigheten, domstolene, og kriminalomsorg i anstalt og frihet.*[35]

I den videre beskrivelsen av samordningsproblemet heter det:

> *En institusjon må ikke få løst sine problemer på en måte som skaper problemer for andre. Da vil det oppstå svake ledd i kjeden, med «køer», svekket effektivitet av rettsapparatet og skadevirkninger både for samfunnet og enkeltmennesket.*[36]

I begrepet strafferettskjede ligger det en erkjennelse av at det ikke hjelper å bare løse et problem ett sted. Likevel er ikke konkrete virkemidler for samordning særlig utførlig behandlet i meldingen. Ulike temaer og ulike involverte etater behandles først og fremst hver for seg, og ikke som ledd i samme kjede.

Betegnelsen strafferettskjeden ble etter relativt kort tid endret til *straffesakskjeden*. Når straffesakskjeden omtales i ulike politiske dokumenter, dreier det seg oftest om de ulike etatenes faktiske oppgaver, og ikke bare

33 Stortingsmelding nr. 23 (1991-92), Om bekjempelse av kriminalitet
34 Hedda Giertsen, Gir den nye kriminalmeldingen «om bekjempelse av kriminalitet» noe nytt om myndighetenes kriminalpolitikk, Lov og rett 1992 s. 478 (særlig s. 486-87)
35 Stortingsmelding nr. 23 (1991-92), s. 10
36 ibid., s. 11

om informasjonsbehandlingen. Straffesakskjeden omfatter «selve» etterforskningen, påtalen, rettssakene og soningen, og ikke bare opplysninger som er avledet av disse handlingene. I denne artikkelen, som handler om registrering og bruk av opplysninger om straff, er det imidlertid primært den informasjonsbehandlingen som er avledet av virksomheten som beskrives.

Problemet med dobbeltregistrering dukker opp igjen – og øker i omfang

Beslutningen om å overføre Strafferegisteret fra Fengselsstyret til Kripos i 1975 innebar endret eieransvar for det formelle registeret. Hvis man tar utgangspunkt i Færdens fire formål med strafferegistrering, ble tre av de fire punktene ivaretatt bedre eller like godt som tidligere. Politiet og påtalemyndigheten fikk raskere og bedre tilgang til kunnskaper om en gjerningspersons tidligere straffer. Oppgavene med å utstede vandelsattester og avgi materiale til statistikkene løses formodentlig like godt uavhengig av hvem som har oppgaven. Det gjensto imidlertid et formål, nemlig kontroll med soningen og kunnskap om eventuelle særskilte tiltak under soning. Flyttingen av registeransvaret førte til at Fengselsstyret mistet et verktøy for egen saksbehandling.

Fengselsvesenet opplevde et behov for teknologistøtte i sin virksomhet. I 1988 begynte Ullersmo fengsel å utvikle et eget lokalt system for administrasjon av soninger. Etter kort tid ble det besluttet å innføre felles edb-verktøy for hele fengselsvesenet, delvis basert på erfaringene fra Ullersmo. Systemet ble kalt «Kompis», og påbegynt rundt 1990. Fra 1996 var Kompis i bruk ved alle fengselsvesenets anstalter.[37]

I Kompis registrerte fengslene blant annet fangers inngang og utgang, ulike tiltak som ble iverksatt, og hendelser under soningen. Inngang og utgang var i prinsippet den samme informasjonen som fengslet skulle melde inn til Strafferegisteret hos Kripos. Kompis bygget opp igjen et «nytt strafferegister» – i hvert fall et system som inneholdt mye informasjon som overlappet med Strafferegisteret – hos Kriminalomsorgsavdelingen i Justisdepartementet. Det var riktignok noe mindre i omfang enn det offisielle Strafferegisteret, ettersom opplysninger om påtaleunnlatelser og lignende ikke ble registrert i Kompis. Bare faktisk iverksatte soninger ble registrert. For de ansatte i fengslene hadde dobbeltregistreringen kommet tilbake, en del av de opplysningene som skulle registreres i Kompis skulle også sendes som meldinger til SSP hos Kripos.

37 Herbjørn Andresen, Om samsvaret mellom et IT-system og et rettslig regelverk, systemdokumentasjon som henviser til rettskilder. Avdeling for forvaltningsinformatikk, Universitetet i Oslo 1999, s. 55

Informasjonsbehandlingen fortsatte å øke i alle involverte etater. Kjernen i strafferettspleiens informasjonsbehov er et straffbart forhold som blir gjenstand for etterforskning, og deretter eventuelt påtale, dom og straffegjennomføring. Derfor vil en god del informasjon om personer og situasjoner være felles for hele sakskjeden. Jo større og mer visjonære perspektiver man velger å anlegge på sammenhenger og muligheter for samordning, jo tydeligere trer overlappingen, dobbeltarbeidet og den manglende samordningen frem.

Fra felles informasjonsmodell til spesialisert arkitektur for samhandling

Kriminalmeldingen fra 1992 hadde omtalt samordningsbehovet i straffesakskjeden. I statsbudsjettet for 1993 omtales justissektorens *informasjonsmodellprosjekt*[38], som er et konkret og systematisk arbeid med å få oversikt over sammenhengene i sektorens informasjonsbehandling. Justisdepartementet utarbeidet en felles informasjonsmodell[39].

I denne informasjonsmodellen ble straffesakskjeden analysert ved hjelp av prosessdiagrammer. Systematikken og notasjonsformen er kjent fra gamle og anerkjente analysemetoder i systemutviklingsfaget. Modellen besto av diagrammer over informasjonsstrømmene både innen hver etat og mellom etatene. Informasjonsstrømmene var tegnet inn og beskrevet uavhengig av hvilke eksisterende informasjonssystemer – elektroniske eller manuelle – som behandlet dem. I tillegg inneholdt modellen en dataordbok, der informasjonstyper er definert. I enkelte situasjoner der to forskjellige organer bruker samme navn på begreper med forskjellig meningsinnhold, ble begge varianter definert slik at behovet for å harmonisere begrepsbruken ble synliggjort. Det var også angitt enkelte referanser til rettskilder, både i prosessbeskrivelsene og i dataordboken, men disse var ikke komplette og gjennomgående.

Ettersom hver av etatene i straffesakskjeden har bygget på eget regelverk og egne informasjonsbehov, utviklet de over tid ulik begrepsbruk og ulike måter å klassifisere fenomener på. Et eksempel, fra 1997-utaven av informasjonsmodellen, er det helt sentrale og tilsynelatende enkle begrepet «lovbrudd». *Definisjonen* av begrepet er den samme gjennom hele straffesakskjeden: «Forhold (handling eller unnlatelse) som etter bestemmelse i lov er belagt med straff»[40]. Likevel ble det operasjonalisert på vidt forskjellige måter i de ulike etatene. Fengselsvesenet opererte med 60 forskjellige formaliserte kodeverdier

38 St. prp. nr. 1, Justis- og politidepartementet, s. 33

39 Informasjonsmodell for straffesaker, dokument G-0230 B, versjon 2.0, Justisdepartementet, Oslo april 1997. Denne versjonen var en omfattende og relativt gjennomarbeidet modell som viste hele sakskjeden, men med en del huller og mangler i detaljbeskrivelsene

40 ibid., s. 167

i Kompis, for å klassifisere ulike lovbrudd. I SSP hos Kripos var det ca. 700 koder som tjente samme formål, altså formodentlig en vesentlig mer finmasket klassifisering. I domsstolenes daværende system ble lovbruddet beskrevet med fri tekst, uten formaliserte koder, under rubrikken «saken gjelder».

Informasjonsmodellen ga en god oversikt over interne grensesnitt og grensesnittene mot andre systemer. Den skulle fungere både som en rettesnor ved utvikling og endring av informasjonssystemer, og som et verktøy for harmonisering av begreper. Begrensningen med en slik modell er imidlertid at den kun analyserer problemet. Senere har Justisdepartementet jobbet mye og lenge med å løse de problemene som informasjonsmodellen bidro til å beskrive, gjennom en bedre integrert elektronisk samhandling.

I en rapport fra en arbeidsgruppe til Justisdepartementet i 2003 ble det foreslått å innføre en «basissak» som et nytt begrep i saksgangen.

> *Basissak defineres som ett straffbart forhold mot en person. Svært ofte vil «saken» som behandles av påtalemyndigheten og domstolene bestå av flere basissaker (funksjonell sak). I og med at en funksjonell sak er bygget opp av flere basissaker vil systemet langs hele straffesakskjeden kunne identifisere hvilke basissaker som er til behandling på de ulike stadier langs prosesslinjen.* [41]

Basissaken er et ektefødt barn av arbeidet med å integrere informasjonsbehandlingen i straffesakskjeden. Det er en tankekonstruksjon som i prinsippet kunne ha vært innført i alle sektorens etater hver for seg, men som da antakelig ville ha vært meningsløs. Det nærmeste man kommer et samsvar med et eksisterende begrep er antakelig «tiltalepunkter» i en sammensatt tiltalebeslutning. Det er først ved samhandling i straffesakskjeden at det er behov for et nytt og mer finmasket atomært nivå for å identifisere enkeltforholdene ved behandling av informasjon om dommer eller straffer.

Man kan spekulere[42] på hvilken eventuell betydning basissak-konstruksjonen kan få for registrering og bruk av opplysninger om straff. Blant de opprinnelig fire formålene med strafferegistrering i Færdens artikkel fra 1899 er det kanskje statistikkproduksjonen som vil bli mest direkte påvirket av en gjennomgående identifisering av basissaker i hele kjeden. Mer finmaskete

41 Elektronisk samhandling i straffesakskjeden: prosessforbedring i straffesakskjeden (DP5), innstilling fra delprosjekt. Rapport avgitt 30. januar 2003, sendt på høring med svarfrist 2. juni 2003

42 Så langt har denne artikkelen vært en liten historiefortelling, med ymse belegg fra skriftlige kilder. Herfra og videre i artikkelen blir det nødvendigvis bare antakelser om effekter av en mulig fremtidig utvikling

grunnbegreper gir større mulighet for presisjon. For eksempel vil man lettere kunne finne ut om samme person ikke bare begår nye kriminelle handlinger, men også om vedkommende dømmes for og eventuelt soner for samme type handling flere ganger.

En annen effekt av å innføre nye grunnbegreper – jeg er fremdeles i avdelingen for noe mer spekulative antakelser – kan kanskje være større oppmerksomhet om detaljer og enkeltforhold, og mindre vekt på helhetsvurderinger, hos de ulike aktørene i straffesakskjeden. For eksempel ville det kanskje være uheldig om fengselsvesenets vurdering av behov for sikkerhetstiltak mot en fange knyttes til erfaringene med ulike typer basissaker, i stedet for å knyttes til en konkret vurdering av den personen det gjelder.

Det noe hypotetiske eksemplet ovenfor dreier seg om en effekt man alltid bør være oppmerksom på i utviklingen av informasjonssystemer: Begrepsfestingen og formaliseringen av informasjonen som behandles kan virke tilbake på den virkeligheten som systemet skal gjenspeile. Man kan ikke uten videre ta for gitt at informasjonssystemene er en nøytral aktør som bare reflekterer en ytre virkelighet.

Jeg vil også ta med en egen, mer vidløftig betraktning om informasjonsbehandlingen i den integrerte straffesakskjeden. I prinsippet vil opplysninger om straff kunne trekkes ut kun fra de dynamiske informasjonsprosessene. Om Strafferegisteret kort og godt fjernes, ligger likevel den samme informasjonen tilgjengelig i den elektroniske samhandlingens ingenmannsland. Den integrerte straffesakskjeden er det langsiktige svaret på de formålene med registrering av straff som Færden formulerte for over hundre år siden. Likevel vil jeg legge til at det neppe er tilrådelig å fjerne det formelle Strafferegisteret, selv om det er teoretisk mulig. Et stabilt register bidrar til institusjonell og regulatorisk tydelighet. Det sørger også for langsiktig kvalitetssikring i den ennå noe teknologisk umodne verden av elektronisk samhandling.

Holder regelverksutviklingen godt nok følge?

Som nevnt innledningsvis, hjemler strafferegistreringsloven både Strafferegisteret som sådan, og ulike aktører i strafferettspleiens bruk av registeret. Likevel er det svært mye som er endret, og som fortsatt vil endre seg, i justissektorens registrering og bruk av opplysninger om straffbare forhold og om straff. Behovet for ny lovgivning er tydelig erkjent, og ble møtt med den omfattende offentlige utredningen med forslag til ny politiregisterlov[43]. Blant de mange forholdene

43 NOU 2003:21, Kriminalitetsbekjempelse og personvern – politiets og påtalemyndighetens behandling av opplysninger

som drøftes er tiltak for å ivareta de registrertes personvern. Det fører altfor langt å presentere forslaget i noen som helst bredde her, men i hovedtrekk kan man si at det legges opp til at politiet i stor grad skal følge helt konkrete regler om håndtering, beskyttelse, korrigering osv. av opplysningene, i stedet for å gi de registrerte noen særlig grad av egen kontroll og medbestemmelse.

Etter utredningen fra 2003 har det vært relativt stille. I Statsbudsjettet for 2007, Justisdepartementets kapitler, er følgende årsak til forsinkelsene oppgitt:

> *Det kan imidlertid se ut som om arbeidet med ny politiregisterlovgivning vil gå langsommere enn planlagt på grunn av regelverksutvikling i EU som er Schengen-relevant. Det fremlagte forslag til rammebeslutning vil kunne få betydning for flere sentrale elementer i den nye politiregisterloven. Det anses derfor ikke hensiktsmessig å videreføre arbeidet med proposisjonen inntil det er nærmere avklart hva som blir resultatet av de pågående drøftelsene i Brussel, der Norge deltar. Det er på det nåværende tidspunkt uklart når disse forhandlingene vil være avsluttet, men det er lite trolig at det vil skje før høsten 2007.*[44]

Det er neppe grunn til direkte å kritisere departementet for å utsette politiregisterloven av slike årsaker. Likevel har det etter mitt syn en noe beklagelig sideeffekt. Det bidrar til at de omfattende endringene i justissektorens informasjonsbehandling blir et mer innadvendt forehavende enn det kanskje burde ha vært. Fremdrift i arbeidet med politiregisterloven ville ha kommunisert viktig informasjon fra departementet om ambisjoner og skranker i dette arbeidet. Regelverksutviklingen og den teknologiske utviklingen bør gå hånd i hånd, men historien om registrering og bruk av opplysninger om straff i Norge viser at regelverksutviklingen dessverre oftest har hengt noe etter.

44 St. prp. nr. 1 (2007-2007) For budsjettåret 2007. Utgiftskapitler: 061, 400-480, Inntektskapitler: 3061, 3400-3474 og 5630, s. 38

ORGANISASJONSENDRING I SIVILSAMFUNNET. TEKNOLOGISK ENDRING OG NYE RETTSLIGE KRAV*

Tommy Tranvik

Innledning

I løpet av de siste 30 årene har norske frivillighetsorganisasjonene gjennomgått en rekke endringer. I forhold til sin tradisjonelle oppbygning, dvs. en liten hovedadministrasjon/sentralnivå tuftet på en stor underskog av selvstendige regionale og lokale foreninger, fremstår dagens organisasjoner på en litt annen måte enn tidligere. Endringene kan, ifølge forskningslitteraturen, oppsummeres i følgende hovedpunkter:

- Sentralisering: antallet ansatte og den årlige omsetningen på sentralt/nasjonalt nivå har økt kraftig. Det samme gjelder omfanget av aktiviteten som er initiert av og skjer med forankring i organisasjonenes hovedkontorer.
- Profesjonalisering: den betalte arbeidskraften har fått en mer fremtredende rolle enn tidligere. Dette gjelder særlig på sentralnivået og i den operative virksomheten utenfor hovedkontoret. Det betyr at organisasjonene er mindre avhengige av den frivillige innsatsen i lokallagene.
- Byråkratisering: veksten i det profesjonaliserte arbeidet, flere administrativt og operativt ansatte og høyere årlig omsetning har ført til at organisasjonene er blitt mer byråkratiserte. Omfanget og betydningen av strategier, handlingsplaner, regler, rutiner og instrukser har derfor økt.
- Statsavhengighet: tidligere var organisasjonene i stor grad egenfinansierte, dvs. at de drev et omfattende inntektsbringende arbeid. Men i løpet av de siste tiårene har nasjonale og lokale myndigheter blitt en stadig viktigere finansieringskilde. Veksten i årlig omsetning og i det profesjonaliserte arbeidet muliggjøres derfor (i stor grad) av offentlige støtteordninger. I

* Denne artikkelen er basert på forskning gjennomført som en del av prosjektet IKT: Utfordringer for demokratisk styring og kontroll, utført ved Rokkansenteret, Universitetet i Bergen. Prosjektet er finansiert via programmet Kommunikasjon, Informasjon og Medier (KIM) i Norges Forskningsråd.

- tillegg har den offentlige reguleringen på områder hvor organisasjonene driver virksomhet tiltatt.[1]

Det er det siste punktet – endrede relasjoner mellom frivillig sektor og staten – og hvilke konsekvenser dette har for (a) utviklingsarbeidet i frivillige organisasjoner og (b) hvordan utviklingsarbeidet påvirker organisasjonenes rolle i det politiske systemet, som fokuset rettes mot her. Med utviklingsarbeid menes i denne sammenheng en bestemt type reforminitiativ som til nå har fått liten oppmerksomhet i den norske frivillighetslitteraturen, men som siden siste halvdel av 1990-tallet i økende grad har definert innholdet i organisatoriske endringsprosesser: e-forvaltningstiltak. E-forvaltningstiltak omfatter investeringer i og bruk av integrerte administrasjonssystemer, dvs. programvare som ivaretar en rekke ulike oppgaver: lønns- og personalsystemer, regnskaps- og økonomistyringsverktøy, medlemsdatabaser, prosjektstyrings-, lager- og arkivsystemer, osv. Hensikten med disse systemene er bl.a. å forbedre frivillige organisasjoners forvaltningskapasitet, profesjonalisere driften og rasjonalisere bruken av ressurser/økonomi.

Hvordan endringer i relasjonene mellom staten og frivillige organisasjoner påvirker utviklingsarbeidet (e-forvaltningstiltak) analyseres med utgangspunkt i empiriske studier av to organisasjoner: Norsk Luthersk Misjonssamband og Norsk Folkehjelp. Her legges det særlig vekt på å klargjøre hvilke interne omstillingsprosesser som sammenhengen mellom nye statlige rammebetingelser og organisasjonenes e-forvaltningstiltak fører til. Det innebærer at fokuset ligger på å vise (a) hvordan organisasjonene jobber for å ivareta nye krav og forventninger fra offentlige myndigheter og (b) hvordan dette arbeidet også er relatert til organisasjonsinterne utfordringer. Kjernepunktene i analysen kan derfor utkrystalliseres på følgende måte:

1. E-forvaltningstiltak handler ikke om tekniske løsninger som implementeres og brukes uten konsekvenser for frivillige organisasjoners oppbygning og virkemåte. Det dreier seg isteden om en ny måte å tenke og praktisere organisasjonsutvikling på. Mens dette arbeidet tidligere omfattet slike ting som medlemsverving, lokallagsutvikling og skolering/kursing av medlemmer og tillitsvalgte, har e-forvaltningstiltak bidratt til at fokuset i økende grad rettes mot systemutvikling, administrativ profesjonalisering og hi-

1 For en mer detaljert gjennomgang av utviklingstendenser i norsk sivilsamfunnsorganisering, se for eksempel Selle og Øymyr 1995; Wollebæk, Selle og Lorentzen 2000; Wollebæk og Selle 2002; Tranvik og Selle 2003 eller Tranvik og Selle 2006.

erarkisk resultatstyring. E-forvaltningstiltak fremstår derfor som en av de viktigste kildene til organisasjonsendring.

2. En avgjørende grunn til denne endringen i fokus kan knyttes til at frivillige organisasjoner utsettes for nye former for eksternt press. Lovpålagte krav til økonomistyring og regnskapskontroll, og evnen til å kunne dokumentere ressursbruk og resultater overfor ikke-statlige donorer (og egne medlemmer), har siden slutten av 1990-tallet i vesentlig grad bidratt til at utviklingsarbeid og e-forvaltningsinitiativ er i ferd med å bli synonyme størrelser. Det betyr at reformtrender i offentlig sektor – spesielt importen av styringsteknikker fra privat sektor – slår inn i frivillige organisasjoner via lovgivningen, og implementeres i form av nye teknisk-administrative løsninger.
3. E-forvaltningstiltak er ikke bare et resultat av eksternt press (nye lovpålagte krav og forventninger fra ikke-statlige donorer), men må også forstås som forsøk på å løse vanskelige interne utfordringer. Spesielt veksten i omsetningen på sentralt nivå og det profesjonaliserte arbeidets økende omfang og kompleksitet, har generert nye behov for intern styring og kontroll. E-forvaltningstiltak har bl.a. til hensikt å gjøre den betalte delen av virksomheten mer styrbar slik at det profesjonaliserte arbeidet foregår med forankring i medlemsbestemte prioriteringer.
4. Siden e-forvaltningstiltakene skyldes kombinasjonen av eksternt press (særlig nye statlige lovkrav) og interne utfordringer (behovet for styring og kontroll), kan konsekvensene sies å være motsetningsfylte. På den ene siden kan det virke som om e-forvaltningsinitiativ signaliserer at frivillige organisasjoner i økende grad behandles som forvaltere av offentlige midler og iverksettere av offentlig politikk. Dette fører trolig til at deres rolle som premissleverandører for offentlige politikk tones ned. På den annen side kan e-forvaltningstiltak bidrar til at organisasjonenes profesjonaliserte arbeid kontrolleres og styres på måter som svekker sannsynligheten for at de ansatte blir den dominerende kraften internt.
5. De motsetningsfylte konsekvensene av e-forvaltningstiltak betyr at mens frivillige organisasjoners eksterne demokratifunksjon ser ut til å svekkes (rollen som premissleverandører for offentlige politikk), kan likevel det organisasjonsinterne demokratiet styrkes (bedre medlemsbasert styring av den profesjonaliserte virksomheten). Det siste betyr trolig at valgte organer på sentralt nivå (styrer og utvalg) styrker sin posisjon sammenliknet med tilsvarende organer på lokalt og regions- eller kretsnivå. Denne vridningen i styrings- og demokratifokus kan innebære større spenninger mellom sentralnivået og lavere organisasjonsnivåer.

Hvorvidt disse argumentene og funnene er representative for frivillig sektor som sådan, er vanskelig å vite. Men det er grunn til å tro at liknende tendenser gjør seg gjeldende i frivillige organisasjoner av tilsvarende størrelse, kompleksitet og profesjonaliseringsgrad som de to som behandles her. Samtidig kan analysen bidra til å kaste lys over noen av mekanismene som ligger bak sentraliserings-, profesjonaliserings- og byråkratiseringstrendene som har vært drøftet i deler av den norske (og nordiske) frivillighetslitteraturen.

Frivillighetslitteraturen og e-forvaltning

I den internasjonale frivillighetslitteraturen finnes det, så vidt vites, få (om noen) studier av e-forvaltningstiltak og utviklingsarbeid i frivillige organisasjoner av den typen som analyseres her. Det henger trolig sammen med at den norske (og nordiske) frivillighetssektoren er spesiell. Mens det i Norge (og Norden) har vært vanlig at nasjonale organisasjoner baserer sin virksomhet på et grunnfjell av lokale foreninger, har det normale i resten av Europa vært en todeling av frivillig sektor. Her har hovedregelen vært nasjonale organisasjoner uten lokallag og lokale organisasjoner uten en nasjonal overbygning.[2] Derfor er det ikke overraskende at e-forvaltningstiltak i organisasjoner av «den nordiske typen» ikke har fått innpass i den internasjonale frivillighetslitteraturen. Isteden kan de fleste studiene av digital teknologi og sivilsamfunn/frivillig sektor deles i fire kategorier:

- Virtuelle samfunn (virtual communities): studier av hvordan elektroniske møteplasser på nettet – som enten er geografisk definert eller tar utgangspunkt i bestemte saker/interesser – benyttes til politiske formål.[3]
- Nye sosiale bevegelser, NGOs og grasrotaktivisme: studier av hvordan løst organiserte og internasjonalt orienterte sammenslutninger, lokale aksjonsgrupper og non-profit organisasjoner benytter digital teknologi i sine aksjoner og kampanjer.[4]

2 Den frivillige sektoren i Nord-Amerika har trolig ligget noe nærmere den nordiske enn den kontinentale organisasjonsmodellen (se Skocpol 2003).

3 Se for eksempel Edwards 2005; Tranvik 2004; Ranerup 2001; Schalken 2000; Tasgarousianou et al. 1998 eller Schalken og Tops 1995.

4 Se for eksempel Burt og Taylor 2007; Van de Donk et al. 2004; Van de Donk og Foederer 2001 eller Hill og Hughes 1998. Se også kapitlet til Christensen og Strømsnes i denne boken.

- Politiske partier: studier av hvordan Internettet og andre digitale teknologier benyttes av politiske partier i interne prosesser, i kommunikasjonen mot omgivelsene (velgere og massemedia) og i valgkampanjer.[5]
- Internettet som en offentlig arena: studier av (og spekulasjoner omkring) i hvilken grad Internettet konstituerer en ny offentlig arena (i konkurranse med bl.a. tradisjonelle massemedia) for politisk debatt og meningsdannelse.[6]

Den mest relevante av disse kategoriene er e-forvaltning og digital teknologi i politiske partier, bl.a. fordi partiene likner på de organisasjonene som studeres her og fordi de baserer deler av sin virksomhet på frivillig innsats. Men partiene er valgkamporganisasjoner som rekrutterer medlemmer til politiske organer innenfor den offentlige styringsstrukturen. Dette gjør dem spesielle i forhold til andre frivillige organisasjoner. Det er heller ikke mye veiledning å hente i den norske (og nordiske) frivillighetslitteraturen. I den grad e-forvaltning og digital teknologi overhode berøres, dreier det seg om organisasjonene har hjemmesider (eller ikke) og om de bruker computere (eller ikke).[7] Denne manglende oppmerksomheten omkring e-forvaltning og digital teknologi, er ikke særskilt for frivillighetslitteraturen. Også forvaltningsforskningen kritiseres for å ha neglisjert teknologiutviklingens betydning for organisasjonsutvikling.[8]

Organisasjonene som analyseres[9]

Organisasjonene som behandles er Norsk Luthersk Misjonssamband (NLM) og Norsk Folkehjelp. Begge er oppbygd på det vi kan kalle den hierarkiske måten:

- Grunnplanet: medlemmer tilknyttet økonomisk og juridisk selvstendige lokalforeninger.[10]

5 Se for eksempel Strandberg 2006; Pedersen og Saglie 2005; Löfgren 2000 eller Delpa og Tops 1995.

6 Se for eksempel Sunstein 2001; Putnam 2000; Keane 2000; Malina 1999 eller King og Kraemer 1998.

7 Se for eksempel Wollebæk og Selle 2002.

8 Se bl.a. Dunleavy et al. 2005: 468-469.

9 Hoveddelen av datainnsamlingen som ligger til grunn for analysene i dette kapitlet, foregikk i perioden november 2004 til mai 2006. Innsamlingen baserte seg på bruk av tre ulike metoder: (1) Deltakende observasjon, dvs. lengre opphold ved de respektive organisasjonenes hovedkontorer, (2) intervjuer med personer som er eller har vært sentrale i organisasjonenes utviklings- og e-forvaltningsarbeid og (3) dokumentanalyser, dvs. gjennomgang av store mengder skriftlig og arkivert materiale. For detaljer om datainnsamlingen og det metodiske opplegget, se Tranvik 2008.

10 Men i NLM forvaltes alle økonomiske verdier i prinsippet av hovedstyret.

- Mellomnivået: lokalforeninger tilknyttet regioner (Norsk Folkehjelp) og kretslag (NLM) som vanligvis er økonomisk og juridisk selvstendige enheter.[11]
- Sentralnivået: demokratisk valgte organer (sentral- og/eller landsstyre) assistert av en sentraladministrasjon ved hovedkontoret.

I tillegg til de tre nivåene, som er ryggraden i organisasjonenes demokratiske styringsstruktur, driver begge organisasjonene ulike typer aktiviteter med utgangspunkt i mellom- og (spesielt) sentralnivået. Dette er det vi kan betegne som den operative delen av organisasjonenes profesjonaliserte virksomhet. I NLM handler det om misjon og bistand, skoler og barnehager, nærmiljøsentre, medievirksomhet og ulike typer selskapsvirksomhet (bl.a. gjenbruksbutikker), mens det i Norsk Folkehjelp primært dreier seg om flyktningmottak og bistands- og mineryddingsarbeid. Den andre delen av det profesjonaliserte arbeidet består i hovedsak av administrasjonen på mellomnivået (krets- og regionskontorer) og de ansatte ved hovedkontoret.

Det religiøse og det sekulære

Selv om NLM og Norsk Folkehjelp representerer forskjellige idéverdener – lavkirkelige lekmannsideologi (NLM) og verdslig solidaritetstenkning (Norsk Folkehjelp) – er de relativt like hverandre når det gjelder satsninger på digital teknologi. I begge organisasjonene er satsningene i stor grad drevet frem av endringer i statlige rammebetingelser (eksternt press), og begge har investert tungt i e-forvaltningssystemer. Det innebærer at strengere statlige krav til bl.a. økonomistyring og regnskapskontroll har lagt føringer på utviklingsarbeidets og teknologiinvesteringenes innretning. Grunnen til dette er at organisasjonene enten mottar store tilskudd fra staten (som i forhold til Norsk Folkehjelps bistands- og mineryddingsinnsats) eller driver utstrakt virksomhet på områder som er regulert og delfinansiert av det offentlige (som i forhold til NLMs bistandsarbeid eller skole- og barnehagedrift). Men, som vi skal se, er likevel erfaringene med og konsekvensene av e-forvaltningstiltak noe forskjellige i NLM og Norsk Folkehjelp.

11 I NLM er det bare lokalforeningene (eller misjonsforeningene) som har rett til å velge representanter til organisasjonens høyeste myndighet – generalforsamlingen. NLM har heller ikke individuelt medlemskap: det er lokallagene (misjonsforeningene) som er «medlemmer» av organisasjonen.

Det religiøse: Norsk Luthersk Misjonssamband

Norsk Luthersk Misjonssamband (NLM) er en selvstendig misjonsorganisasjon som er tilsluttet Den Norske Kirke. Organisasjonen ble stiftet i 1891, og driver misjons- og bistandsarbeid i 15 land. NLM skiller seg fra andre kristne misjonsorganisasjoner i Norge ved at ytremisjonsarbeidet kombineres med et svært ambisiøst og sammensatt arbeid i Norge. Organisasjonen hadde i 2005 en årlig omsetning på ca. 900 mill. kr. fordelt på 180 ulike enheter, institusjoner og selskaper, både i Norge og i utlandet. Disse enhetene ansatte noe i overkant av 3000 medarbeidere. I tillegg er omkring 2700 lokalforeninger og 22 forsamlinger tilsluttet organisasjonen.[12]

E-forvaltningstiltakene i NLM representerer én av de tre største omstillingsprosessene som organisasjonen har gjennomgått siden den ble stiftet.[13] Tiltakene omfatter etableringen av tvillingselskapene NLM IKT Service A/S og NLM Økonomiservice A/S.[14] I 2005 forvaltet tvillingselskapene til sammen 52 årsverk og hadde en samlet omsetning på nesten 35 mill. kr. Mandatet som tvillingselskapene ble utstyrt med, var å sørge for at alle enheter (foreninger, kretser, misjonsfelt, institusjoner og selskaper) tok i bruk de samme teknologisystemene og at mesteparten av regnskaps- og økonomiarbeidet i organisasjonen ble overført til NLM Økonomiservice. Hensikten med e-forvaltningstiltakene var derfor å profesjonalisere og sentralisere det teknisk-administrative arbeidet og rasjonalisere organisasjonsdriften. Dermed skulle NLMs enheter, institusjoner og selskaper brukte mindre tid og ressurser på administrasjon og mer på deres kjerneoppgaver (skolene skulle konsentrere seg om skolefaglig kompetanseutvikling, lokalradioene om å lage gode radioprogrammer, misjonsfeltene om å formidle det kristne budskapet, osv.). I tillegg var det en viktig forutsetning at det høyeste medlemsvalgte organet – hovedstyret – fikk bedre oversikt, styring og kontroll med den omfattende og kostnadskrevende profesjonaliserte virksomheten i Norge og utlandet.

Bakgrunnen for opprettelsen og oppbyggingen av NLM IKT Service og NLM Økonomiservice – og målsetningen om sterkere overordnet styring av det profesjonaliserte arbeidet – går tilbake til begynnelsen av 1980-tallet. Det

12 Se Årsmeldingen 2005.

13 De to andre store omstillingsprosessene er knyttet til (a) satsningene på egen institusjons- og selskapsdrift (som startet med etableringen av organisasjonens misjonsskole på slutten av 1890-tallet, og som nå omfatter en rekke andre institusjoner og selskaper), og (b) ekspansjonen i ytremisjonsarbeidet i årene fra 1949 og fremover.

14 Begge selskapene er 100 % NLM-eide. Frem til sommeren 2005, var NLMs hovedstyre generalforsamling for både NIS og NØS. Nå er aksjene i selskapene overført til NLMs eiendomsselskap (NLM Eiendom A/S), noe som innebærer at styret i eiendomsselskapet er tvillingselskapenes nye generalforsamling.

skyldes at visse problematiske utviklingstendenser har preget NLM i løpet av de siste 20–25 årene:

- Antallet lokalforeninger tilsluttet NLM er redusert med omkring 1000 siden begynnelsen av 1980-tallet.
- Veksten i gaveinntektene bremset opp i løpet av 1990-tallet, og greide ikke å holde tritt med den generelle kostnadsutviklingen i samfunnet.
- Misjonærtallet er redusert til mindre enn 1/3 av hva det var i 1980, og antallet forkynnere i Norge er vesentlig mindre enn for 25 år siden.
- Abonnementstallet for organisasjonsavisen Utsyn er redusert fra omkring 42 000 i 1980 til ca. 14 200 i 2005.[15]

Disse utviklingstendensene førte til et økende behov for å omorganisere og rasjonalisere organisasjonsarbeidet – forståelsen for at «noe måtte gjøres» modnet i organisasjonen. Men det var først da det eksterne presset på NLMs administrasjonsordninger økte i siste halvdel av 1990-tallet, at utviklingsarbeidet kom til å omfatte e-forvaltningstiltak.

Det eksterne presset går tilbake til begynnelsen av 1990-tallet. Frem til 1992 hadde de frivillige organisasjonene en relativt fri stilling i forhold til skatteregimer og regnskapsføring. Men i forbindelse med skattereformen som Stortinget vedtok i 1992, ble det klart at NLMs hovedkasse måtte føre sine regnskaper i henhold til den daværende regnskapsloven. Dette innebar bl.a. at NLMs hovedkasse (som omfatter hovedkontoret, lokalforeninger, kretser og misjonsfelter) måtte legge om måten regnskapet ble ført på. Den viktigste omleggingen var at organisasjonen måtte bruke regnskaps- istedenfor kontantprinsippet.[16] Kontantprinsippet betyr at utgifter og inntekter regnskapsføres etter hvert som penger tjenes eller brukes. Dermed fremgår balansen av kontoutskriften. Regnskapsprinsippet innebærer derimot at de faktiske verdiene i organisasjonen skal regnskapsføres, bl.a. eiendommer, utstyr, «frynsegoder», osv. Samtidig skal investeringskostnader (for eksempel utgifter til kjøp av PC) fordeles over investeringens levetid (i henhold til kontantprinsippet, regnskapsføres utgiften til kjøp av ny PC når den betales).[17]

Konsekvensen av overgangen fra kontant- til regnskapsprinsippet var bl.a. at regnskapsføringen ble langt mer komplisert, regelstyrt og ekspertintensiv

15 For en mer detaljert oversikt over disse utviklingstrekkene, se særlig NLMs årbøker (dvs. årsmeldingene) for perioden 1980 til 2005.

16 Birger Helland, forretningsfører hovedkassen, intervju 01.06.05.

17 Regnskapsprinsippet har vært vanlig i privat næringsvirksomhet. Krav om bruk av regnskapsprinsippet i frivillig sektor er et eksempel av at organisasjoner i økende grad kommer inn under regler som tidligere bare gjaldt i næringslivet.

enn hva den hadde vært tidligere – økonomi og regnskapsarbeidet ble byråkratisert:

> *«Til sammen betyr dette at administrasjonen i frivillige organisasjoner blir større og større, og det kan føre til at gründertypene forsvinner. Vi merker dette veldig godt i NLM. Informasjonskravene øker i alle fall annethvert år slik at mye av organisasjonsutviklingen i NLM skyldes nye krav fra offentlige myndigheter (…) Men det er ikke bare offentlige myndigheter som stiller strengere krav til NLM. Vi har sett en klar tendens til at giverne ønsker å kunne følge hvordan pengegavene brukes i misjonens tjeneste (…) Dette fører til mindre budsjettfleksibilitet og stiller større krav til de administrative systemene.»*[18]

Ifølge denne oppfatningen, utsettes NLM for et dobbelt administrasjonspress: fra offentlige myndigheter (staten) og fra ikke-statlige donorer. Likevel er det kravene fra myndighetene som har størst innvirkning på organisasjonsutviklingen.

For å ivareta de nye regnskapsføringsreglene, ble NLM Økonomiservice A/S etablert (med én ansatt) i 1995. Men seks år senere – i 1998 – ble en ny regnskapslov vedtatt. Ifølge denne loven, skulle det samme regnskapsregimet som fra 1992 bare omfattet hovedkassen nå også gjelde for NLMs øvrige enheter, selskaper og institusjoner (skoler, barnehager, leirsteder, lokalradiostasjoner, osv.). I etterkant av 1998-loven, kom det i tillegg en rekke nye lover som skjerpet og byråkratiserte kravene til økonomistyring og regnskapskontroll ytterligere: merverdiavgift på tjenester (2001), nytt regelverk for NORAD (2002), revisjon av regnskapsloven (2003), revisjon av skatteloven (2003), ny bokføringslov (2005) og ny skattereform (2005).

Revisjonen av skatteloven i 2003, kan tjene som eksempel på hvordan lovverket vanskeliggjør administrasjonsarbeidet i NLM. Tidligere var det ikke krav om innbetaling av arbeidsgiveravgift for misjonærer på feltene, og det var andre regler enn i dag for beskatning av misjonærlønninger. Men med lovendringen i 2003, må ikke bare misjonærlønningene, men også verdien av eventuelle frynsegoder (gratis bolig, bil, penger til livsopphold, osv.) rapporteres. Spørsmålet er hvordan frynsegodene skal verdsettes: hva er verdien av et hus midt ute i den afrikanske bushen hvor det ikke finnes noe boligmarked? Den samlede virkningen hevdes derfor å være at det må gjøres stadig mer komplekse og kompetansekrevende vurderinger for å oppfylle skatte- og regnskapsreglene, og at det må rapporteres mer sammensatt informasjon til flere

18 Edvin Håvik, daglig leder i NLM Økonomiservice, intervju 22.04.05.

interessenter enn tidligere (myndigheter, banker, leverandører, ansatte, givere, kretser, misjonsfelter, institusjoner, bedrifter, osv.).

Som en følge av denne utviklingen, ble det stilt stadig høyere krav til NLMs e-forvaltningsverktøy, særlig regnskaps- og økonomistyringsprogrammer.[19] NLM IKT Service ble derfor etablert i 2002 for å sikre at teknologien som var nødvendig for lovmessig føring av organisasjonens omkring 300 ulike enkeltregnskaper kom på plass. Målet med selskapsdannelsen var derfor å implementere e-forvaltningssystemer som ivaretok kravene i den nye lovgivningen i en situasjon hvor organisasjonen i utgangspunktet var preget av en rekke bekymringsfulle utviklingstrekk.

Ny teknologi, endret arbeidsdeling og interne konflikter

Ovenfor har vi sett at det ble oppfattet som nødvendig å profesjonalisere teknologiarbeidet for å imøtekomme de nye lovkravene.[20] Profesjonaliseringen skjedde med utgangspunkt i en kartlegging av teknologitilstanden i NLM. Denne viste at tilstanden i deler av organisasjonen nærmet seg krise, at det var stort behov for å rydde opp i mangfoldet av teknologier som ble benyttet og at NLM manglet e-forvaltningssystemer som kunne imøtekomme de nye lovkravene som ble stilt til økonomistyring og regnskapsføring. Innholdet i kartleggingen ga støtet til, og dannet bakgrunnen for, utarbeidelsen av en IKT-strategi for hele NLM: et dokument som ble fremlagt og godkjent av NLMs hovedstyre i september 2001. Hovedpunktene i den relativt omfattende strategien var at digital teknologi skulle brukes til å bygge en mer helhetlig og effektiv organisasjonsstruktur, og at IKT-ansvaret skulle overføres fra lokale enheter til NLM IKT Service. Dokumentet beskrev også hvilke tiltak som var nødvendige innenfor de forskjellige virksomhetsområdene – misjonsfelt, skoler, barnehager, leirsteder, osv. – for skape en mer helhetlig og effektiv administrasjonsordning. Tanken var at den programvaren som kretser, misjonsfelt, institusjoner og selskaper hadde bruk for skulle ligge på sentrale servere ved hovedkontoret og at de ulike enhetene skulle ha tilgang til serverne over raske telesamband.[21] Dermed skulle lokale enheter ikke ha behov for å kjøpe og drifte egne programmer for administrativ databehandling.[22]

19 Edvin Håvik, daglig leder i NØS, intervju 29.05.05.
20 Strategi og visjonsdokument for IKT i NLM (2001), s. 5.
21 Det har derfor blitt bygd opp en stor serverpark ved organisasjonens hovedkontor på Sinsen i Oslo.
22 Tore Marthinsen, daglig leder i NIS, intervju 20.03.06.

Samtidig skulle de nye e-forvaltningssystemene gjøre det mulig for NLM Økonomiservice å overta arbeidet med regnskapsføringen i hele NLM.[23] NLM IKT Service fikk dermed ansvaret for de teknologiske løsningene, mens NLM Økonomiservice skulle tilby de viktigste tjenestene som løsningene ivaretok. Hvordan alt dette skulle skje – innenfor hvilke budsjett- og tidsrammer – og på hvilken måte hovedstyret skulle ivareta sitt styringsansvar, var imidlertid spørsmål som ble hengende i luften. Bortsett fra å godkjenne IKT-strategien og å opprette NLM IKT Service hadde ikke hovedstyret lagt en plan for hvordan implementeringsarbeidet skulle utføres. Disse spørsmålene overlot hovedstyret til selskapene selv å ta stilling til.

Utfordringen som tvillingselskapene støtte på da de startet implementeringsarbeidet, var at de stod overfor en del store og tunge institusjoner som hadde basert sin drift på «teknisk-administrativ sjølberging»: de hadde vært vant til å ivareta dette arbeidet uten innblanding fra sentralt hold. Det innebar at de enten på egen hånd eller i samarbeid med lokale selskaper (IT- og regnskapsføringsselskaper) hadde bygd opp en selvstendig teknisk og administrativ kapasitet. Det de nå fikk vite var at denne selvstendigheten ikke lenger var forenlig med NLMs IKT-strategi: teknologivalg samt økonomi- og regnskapsføringsarbeidet skulle overlates til to nye selskaper. Selv om mange av NLMs kretser, bibelskoler og leirsteder så positivt på at de fikk kvalifisert hjelp til å løse vanskelige administrasjonsoppgaver, var mange av NLMs skoler skeptiske til konsekvensene av IKT-strategien: vil vi miste trofaste medarbeidere på økonomi-, regnskaps- og teknologisiden; må vi si opp avtaler med lokale IT- og regnskapsføringsselskaper; vil vi få like god service fra tvillingselskapene som fra våre lokale samarbeidspartnere; vil selskapene tre standardiserte løsninger ned over hodene på oss; vil vi motta en strøm av dyre regninger fra sentralt hold; vil vi miste styringen over egen virksomhet når det teknisk-administrative arbeidet overtas av NLM IKT Service og NLM Økonomiservice?

I tillegg til disse bekymringene, stilte enkelte røster spørsmålstegn ved teknologivalgene til NLM IKT Service. Det ble for eksempel hevdet at økonomistyrings- og regnskapsverktøyet (Oracle Financials) hadde mange funksjoner som skolene ikke hadde bruk for. Dermed ble programvaren veldig tungt å jobbe med.[24] Samtidig var det en viss usikkerhet knyttet til om NLM Økonomiservice hadde god nok kapasitet til å føre regnskapene for de største skolene. Andre skoler var misfornøyde med at selskapets kontoplaner var for store og komplekse i forhold til deres behov. Det ble også uttrykt misnøye

23 Edvin Håvik, daglig leder i NØS, intervju 22.04.05.

24 Sveinung Kjosavik, administrasjonssjef på Tryggheim Skoler, Nærbø på Jæren, intervju 23.03.06.

med prisen som selskapene tok seg betalt for å utføre sine tjenester. Dette er likevel detaljinnvendinger i forhold til den grunnleggende problematikken som teknologisatsningene reiste: hvordan flytte viktige arbeidsoppgaver fra lokale til sentrale enheter i en organisasjon basert på sterke tradisjoner for lokal selvstendighet og «teknisk-administrativ sjølberging»? Hvordan skal tvillingselskapene ivareta sine oppgaver innenfor en slik kontekst?

Disse spørsmålene ble etter hvert så problematiske og påtrengende at NLMs hovedstyret nedsatte en evalueringsgruppe for NLM IKT Service og NLM Økonomiservice i juni 2005. Gruppen fikk i oppgave å utrede alle sider ved tvillingselskapenes implementering av IKT-strategien. Konklusjonene ble presentert i en omfattende rapport fremlagt på hovedstyremøtet i mai 2006. I rapporten hevdes det at tvillingselskapene hadde møtt skepsis og motstand utover i deler av organisasjonslandskapet på grunn av sviktende overordnet styring: hovedstyret burde spilt en mer aktiv rolle i å forklare hvorfor det var nødvendig at alle NLMs enheter benyttet seg av selskapenes tjenester. Rapporten hevder likevel at misnøyen med tvillingselskapene ikke var så stor som enkelthenvendelser adressert til hovedstyret, hovedkontoret eller selskapene selv kunne tyde på. Utfordringen som rapporten beskriver, er at i en organisasjon hvor den lokale selvstendigheten nærmest står på bibelsk grunn, er det ekstra viktig at den øverste ledelsen kommuniserer tydelig hva den ønsker å oppnå med de tiltakene den iverksetter.[25] Spesielt avgjørende er dette når tiltakene går ut på å endre arbeidsdelingen mellom lokale og sentrale enheter. Problemet, ifølge evalueringsrapporten, var at tvillingselskapene manglet den nødvendige autoriteten til å gjøre jobben sin på en effektiv måte. Denne autoriteten var det et passivt hovedstyre som satt med.

Demokratisynets motsetningsfylte logikk

Rapporten peker også på at ledelsen i NLM i for liten grad tok inn over seg at e-forvaltningstiltakene utfordret grunnfestede oppfatninger om hvordan organisasjonen bør være oppbygd og fungere. Disse oppfatningene er kjernen i NLMs demokratisyn, og uttrykkes med stor tyngde av organisasjonspioner og tidligere generalsekretær Ludvig Hope:

> *«Etter hvert som ei vekkjingsrørsle vinn makt og folkegunst og vert stor, kjølnar ho av, vert mindre fanatisk og pietistisk, og ho missar odd og egg og*

25 Se Godt begynt er halvt fullendt. Rapport fra Evalueringsgruppen for NLM Økonomiservice A/S og NLM IKT Service A/S. Fremlagt på hovedstyremøtet 12.-13. mai 2006.

kraft (…) Og når den indre krafta minkar, prøver ein å halde seg oppe med ytre oppussing. Ein lagar bod og reglar og ritual, fine hus og kunst.»[26]

Det som her formidles er at det ikke bør brukes store ressurser på administrasjon og byråkratiske ordninger. Isteden er det overbevisningskraften som springer ut av medlemmenes tro på saken som skal være bærebjelken i arbeidet. Denne overbevisningskraften kommer først og fremst til uttrykk i misjonsforeningene (lokallagene) – det er på grunnplanet at organisasjonen skal vinne terreng for sin sak. Dermed legges en klar føring på arbeidsdelingen mellom organisasjonsnivåene: grunnplanet må kunne drive sin virksomhet uten særlig innblanding fra overordnede organer. Kritikerne kan derfor tolkes som forsvarere av den tradisjonelle «demokratiske orden» – innflytelse utøves gjennom det daglige arbeidet i lokale enheter, institusjoner og selskaper – og frykten var at hovedstyret ville bruke e-forvaltningsverktøyene (og tvillingselskapene) til å sentralisere styringen av ressurser og prioriteringer.

Men i tillegg til skepsis mot sentralisering, er NLMs demokratisyn tuftet på en annen og motstridende oppfatningen – lavere nivåer må vise lojalitet overfor ledelsen:

«Vi skal beflitte oss på å underkaste oss den organisasjonen vi tjener, men gjør det etter denne regelen: Vær organisasjonsledelsen til behag på en slik måte at vi ikke vekker Herrens mishag.»[27]

Det er først og fremst i teologiske spørsmål at man har et ansvar for å vurdere om ledelsens synspunkter står på trygg grunn. I andre spørsmål, er utgangspunktet at man i størst mulig grad bør bestrebe seg på å følge de vedtak som demokratisk valgte organer har fattet.[28] Derfor kan det se ut som om spenningen mellom demokratisynets to grunnpilarer – lokal selvstendighet vs. ledelseslojalitet – ble satt på spissen (i alle fall i deler av organisasjonsapparatet) da IKT-strategien skulle implementeres. Denne spenningen ble trolig forsterket av ledelsen passivitet: fra ledelsens side ble lojalitet tatt for gitt, men dette førte til at de lokale enhetene ble dårlig informert om hva vedtakene betydde for dem. Dermed var det uklart hva det var de ble bedt om å være lojale overfor.

26 Sitert på s. 174 i Veien Fram. Grunnsyn og arbeidsmåter i Norsk Luthersk Misjonssamband (1977). Oslo: Lunde Forlag.

27 Øivind Andersen, tidligere «organisasjonsideolog» og rektor på Fjellhaug Misjonsskole, sitert på side 45 i Veien Fram. Grunnsyn og arbeidsmåter i Norsk Luthersk Misjonssamband (1977). Oslo: Lunde Forlag.

28 Det sentraliserende elementet i NLMs ideologi understøttes av at hovedstyret i prinsippet er ansvarlig for forvaltningen av organisasjonens økonomi og eiendom.

Skepsisen som e-forvaltningstiltakene ble møtt med i deler av NLM, er likevel ikke et uttrykk for at satsningene har havarert. I 2006 benyttet for eksempel 80 % av NLMs enheter seg av tjenestene som NLM Økonomiservice tilbyr (økonomistyring, regnskapsføring og rådgivning).[29] Når det gjelder NLM IKT Service, er det vanskeligere å gi en liknende statusrapport. Men selv om selskapet i 2006 leverte produkter eller rådgivningstjenester til nesten alle NLMs enheter, er det langt igjen til målsetningen om at selskapet skal være hovedleverandør av teknologitjenester i NLM.

Det sekulære: Norsk Folkehjelp

Utviklingen i Norsk Folkehjelp som fører frem til organisasjonens e-forvaltningstiltak henger nøye sammen med den som er skissert i NLM – eksternt press har vært avgjørende. Men som i NLM har interne og problematiske utviklingstrekk gjort organisasjonen moden for omstilling. Samtidig er e-forvaltningssatsningene i Norsk Folkehjelp av et langt mindre omfang enn i NLM.

Norsk Folkehjelp ble stiftet i 1939, og er fagbevegelsens humanitære bistandsorganisasjon (men har ingen formell tilknytning til noen politiske partiene).[30] Norsk Folkehjelp driver et bredt sammensatt arbeid i Norge og utlandet. Utenlandsinnsatsen omfatter langsiktig bistandsarbeid og minerydding i over 30 land, mens den hjemlige innsatsen konsentrerer seg om førstehjelps- og redningsarbeid, drift av flyktningmottak og frivillighetssentraler, integrasjonsarbeid i forhold til innvandrere og holdningsskapende kampanjer (i særlig grad anti-rasistisk arbeid). Organisasjonen hadde i 2005 omkring 12 500 medlemmer.[31] Likevel var det årlige omsetning på imponerende 770 mill. kr. og organisasjonen hadde i underkant av 3000 ansatte.[32] Norsk Folkehjelps medlemsorganisasjon er derfor svært liten sammenliknet med størrelsen på det profesjonaliserte arbeidet.

Årsakene til skjevheten mellom medlemsdelen og den profesjonaliserte aktiviteten strekker seg tilbake til begynnelsen av 1980-tallet: I 1983 var Norsk Folkehjelp for første gang vertskap for NRKs årlige tv-innsamlingsaksjon.[33]

29 Se evalueringsrapporten Godt begynt er halvt fullendt (2006).

30 Se bl.a. Solidaritet. Norsk Folkehjelps prinsipper og verdigrunnlag (2003).

31 Norsk Folkehjelps tilknytning til LO innebærer at alle LOs medlemmer er kollektivt innmeldt i Norsk Folkehjelp (og LO er representert i organisasjonens nasjonale styre). Hver LO-medlem bidrar med tre kroner av fagforeningskontingenten til Norsk Folkehjelps arbeid.

32 Se Årsrapporten 2005. De fleste – ca. 2400 – er lokalt ansatte i utlandet som driver med minerydding.

33 Laila Nikolaisen, tidligere leder i Internasjonal Avdeling, intervju 29.09.05.

Dette, sammen med beslutningene i 1988 og 1992 om å starte drift av flyktningmottak i Norge og å satse på minerydding i utlandet, førte til at den årlige omsetningen, antallet ansatte og aktivitetsspektret økte dramatisk. Veksten i virksomhetsomfanget kan illustreres ved hjelp av følgende nøkkeltall:

- I 1990 var den årlige omsetningen på i 226,2 mill. kr. Den steg til 431,6 mill. kr. i 1994, 633,3 mill. kr. i 1996 og videre til 731,4 mill. kr. i 2000.
- Omsetningen i det internasjonale arbeidet steg fra 177 mill. kr. i 1990 til 525 mill. kr. i 2000.
- Det totale antallet ansatte steg fra 195 i 1991 til 2777 i 2001.
- Antallet ansatte ved hovedkontoret i Oslo økte fra 31 i 1987 via 98 i 1995 til 136 i 2000.[34]

Problemet var at utviklingen av forvaltningskapasiteten holdt ikke følge med veksten i det profesjonaliserte arbeidets omfang og kompleksitet. Samtidig befant organisasjonen seg i en utsatt økonomisk stilling – egenkapitalen utgjorde bare noen få prosent av omsetningen. Dermed risikerte Norsk Folkehjelp store problemer hvis økonomistyringen kom ut av kontroll innenfor ett eller flere av de store bistands- eller mineryddingsprogrammene. Særlig regnskapstallene for budsjettåret 2000 satte en støkk i organisasjonen: Norsk Folkehjelp endte opp med et underskudd på 11 mill. kr. og tapt egenkapital. Dermed stod det klart for ledelsen at investeringer i nye e-forvaltningssystemer var avgjørende for å unngå at organisasjonen havnet i en tilsvarende situasjon i fremtiden.

På toppen av veksten i løpet av 1980- og 1990-tallet (og den økonomiske usikkerheten som veksten førte med seg), kom kraftig eksternt press. Som i NLM, var det eksterne presset knyttet til skjerpede statlige krav til økonomistyring og regnskapskontroll. Endringer i regnskapsregimet som regnskapsloven av 1998 innebar, er for eksempel noe som også Norsk Folkehjelp må forholde seg til. Det samme gjelder nytt regelverk for NORAD (2002), revisjon av regnskapsloven (2003), ny bokføringslov (2005) og ny skattereform (2005).

Skjerpede krav og forventninger fra offentlige myndigheter (særlig fra NORAD og Utenriksdepartementet) og ikke-statlige donorer om administrativ profesjonalisering er ikke av ny dato. Som i forhold til NLM, strekker kravene og forventningene seg tilbake til tidlig på 1990-tallet, og utløste fra tid til annen frustrasjon i organisasjonens ledelse. Denne frustrasjonen kom bl.a. til uttrykk på landsmøtet i 1995:

34 Se Norsk Folkehjelps årsrapportene for perioden 1979 til 2000.

«Vi godtar og setter pris på at det vi gjør blir kontrollert. Det vi imidlertid ikke kan akseptere, er byråkratisk kontroll som bidrar til å lamme det arbeidet vi skal gjøre for dem som har det vanskeligst og er rammet av krig, ulykker og forfølgelse.»[35]

Frustrasjonen henger bl.a. sammen med den endrede rollen som bistandsorganisasjonene (inkludert Norsk Folkehjelp) spilte i forhold til norske myndighetsdonorer på 1990-tallet. På 1980-tallet var det for eksempel vanlig at organisasjonene søkte Utenriksdepartementet (UD) om midler til egendefinerte prosjekter. Men utover på 1990-tallet ble det stadig vanligere at organisasjonene måtte søke midler på prosjekter definert av UD selv.[36] Konsekvensen hevdes å være at Norsk Folkehjelp i større grad enn tidligere fikk rollen som iverksetter av andres (istedenfor egnes) ideer og målsetninger.[37] Dette krevde mer operativ kapasitet og kompetanse, og førte til mindre oppmerksomhet omkring den politiske eller ideologiske motivasjonen for organisasjonens virksomhet.[38] Samtidig innebar rolleendringen at kravene til rapportering og kontroll ble skjerpet: når du i tillegg til å forvalte andres penger også skal implementere deres ideer og målsetninger, øker donors interesse for informasjon om hvordan arbeidet utføres og hvilke resultater som oppnås. Og utover på 2000-tallet har kravene til økonomistyring og rapportering blitt ytterligere innskjerpet. Dette gjelder nesten alle typer donorer. For eksempel har NORAD skjerpet sine revisjonskrav betydelig, men kravene kommer også fra Riksrevisjonen: «(…) det blir stadig mer revisjon»:[39]

«UD, FN og andre donorer stiller strengere krav til tilbakerapportering og økonomistyring. Dette fører til økende behov for profesjonalisering og kapasitetsoppbygging.»[40]

---

35 Harald Øveraas, daværende styreleder, i tale til landsmøtet 16. juni 1995 (manus vedlagt Protokoll for landsmøtet 1995).

36 Denne utviklingen berører ikke NORAD. Her er det fortsatt slik at organisasjonene får penger til egendefinerte prosjekter. Det betyr at i forhold til NORAD-finansierte prosjekter, skjer evalueringer av bistandsarbeidet med utgangspunkt i Norsk Folkehjelps egen målsetninger for prosjektarbeidet.

37 Per Ranestad, seksjonsleder i Internasjonal Avdeling, intervju 18.11.05.

38 Norsk Folkehjelps innsats på Balkan tidlig på 1990-tallet beskrives av enkelte som et eksempel på mindre politisk begrunnet bistandsengasjementet: Norsk Folkehjelp drev virksomhet i området – ikke fordi organisasjonen støttet noen av partene – men fordi det var en konflikt der, og fordi det var enkelt å få finansiering til prosjekter.

39 Eli Voksø, administrasjonssjef, intervju 05.12.05.

40 Protokoll fra sentralstyremøtet 18.06.93.

Dette har ført til behov for investeringer i e-forvaltningssystemer som er i stand til å levere de rapportene og regnskapsoversiktene som lovgivningen og ikke-statlige donorer krever eller forventer.

Men samtidig med at det stilles strengere administrasjonskrav fra norske myndigheter, har Norsk Folkehjelp en rekke internasjonale donorer som opererer med egne rapporterings- og kontrollrutiner. Spesielt viktig i denne sammenheng er USAID – USAs motsvarighet til NORAD – som er Norsk Folkehjelps klart største utenlandske donor.[41] I tillegg til at en rekke betingelser knyttes til pengene som Norsk Folkehjelp mottar fra USAID (for eksempel at korn til Sør-Sudan må fraktes på amerikanske båter og lastebiler), må organisasjonen godtgjøre krav på dekning av egne administrasjonskostnader i forbindelse med forvaltningen av støtten fra amerikanerne. Hvilke administrative kostnader Norsk Folkehjelp kan få dekket, er spesifisert i den såkalte NICRA-avtalen.[42] Den innebærer at alle utgifter som Norsk Folkehjelp ønsker refundert (og som er spesifisert i NICRA), må klassifiseres (direkte eller indirekte kostnader) og dokumenteres på prosjektnivå. Men det forutsetter at man både har interne rutiner og teknologiske løsninger som gjør klassifisering og dokumentering mulig. Norsk Folkehjelp har i mange år ikke hatt slike systemer. Dermed har organisasjonen tapt penger på å motta støtte fra USAID.

Concorde settes på bakken og Agresso tar over

Som i NLM, dreier e-forvaltningstiltakene i Norsk Folkehjelp seg om endring av arbeidsdelingen mellom hovedkontoret og underliggende organisasjonsnivåer og enheter, spesielt organisasjonens 15 utenlandskontorer (disse kontorene administrerer bistands- og mineryddingsinnsats). Og, som i NLM, dreier det seg om implementering av nye teknologisystemer (særlig økonomistyrings- og regnskapsføringsprogrammer) som skal gjøre det lettere å imøtekomme nye lovpålagte rapporteringskrav og å administrere den store og sammensatte program- og prosjektportefølje på en hensiktsmessig måte.

Med økonomikrisen fra 2000/01 friskt i minne, vedtok Norsk Folkehjelp en ny IKT-strategi i 2003.[43] Det viktigste punktet i strategien var anskaffelse og

41 USAID støttet Norsk Folkehjelp med 134,2 mill. kr. i 2005 (Årsrapporten 2005). Alle disse pengene gikk til organisasjonens arbeid i Sør-Sudan.

42 NICRA = Negotiated Indirect Cost-Rate.

43 Organisasjonen kom seg ut av krisen i 2000 ved å redusere bemanningen ved hovedkontoret (fra 136 til 94 ansatte). Nedbemanningsprosessen foregikk fra slutten av 2001 til begynnelsen av 2003. Samtidig ble det bestemt at Norsk Folkehjelp skulle utføre mineryddingsoppdrag på vegne av Norsk Hydro i Iran – en kontrakt som var verdt i overkant av 40 mill. kr.

implementering av et nytt e-forvaltningssystem for hele organisasjonen. Dette arbeidet – den såkalte Agresso-prosessen (som foregikk fra 2003 til 2005) – førte til at Norsk Folkehjelp byttet ut det gamle e-forvaltningssystemet – IBMs Concorde – som organisasjonen hadde brukt siden 1995 (se nedenfor).

På tilsvarende måte som i NLM, beskrives tilstanden på IT-området i Norsk Folkehjelp som til dels kaotisk i årene før 2003-strategien ble vedtatt:

> *«Frem til IT-strategien ble vedtatt, florerte det med programmer i Norsk Folkehjelp. Mange av dem var lastet ned fra Internettet fordi noen hadde en svoger som mente at det ene eller andre programmet var kjekt å ha. Det fantes ingen systematisk tenkning i forhold til hva man trengte av IT-hjelpemidler eller hva som var fornuftig å gjøre på dette området.»*[44]

Denne uoversiktlige tilstanden reflekterte – i alle fall til en viss grad – tenkningen som lå til grunn for Norsk Folkehjelps første IT-strategi, vedtatt i 1994. I det korte strategidokumentet heter det bl.a. at Norsk Folkehjelp er en desentralisert organisasjon med felles sentraladministrasjon: «Vi har derfor valgt en desentral datastrategi, dvs. at hvert utekontor og asylmottak og liknende kan ha sine data lagret lokalt.»[45] Konsekvensen av denne tenkningen – lokal kontroll med lokale data – var manglende samordning av IT-ressurser og kompetanse: hver lokal enhet stod relativt fritt til selv å velge hva den ville gjøre på IT-området. Likevel ble det på midten av 1990-tallet gjennomført én stor og felles IT-satsning: anskaffelsen av e-forvaltningssystemet Concorde. Grunnen til anskaffelsen var at vekstperioden som organisasjonen på denne tiden befant seg i førte til behov for nye og kraftigere administrasjonsverktøy.

Helt fra starten av var Concorde plaget med problemer. Norsk Folkehjelp fikk for eksempel ikke lønns- og personalmodulene til å fungere skikkelig (til slutt valgte organisasjonen å investere i lønns- og personalsystemet fra selskapet Huldt & Lillevik). Samtidig tok implementeringen av Concorde på utekontorene svært lang tid. Mens systemet ble tatt i bruk ved hovedkontoret i januar 1995, var det ved utgangen av 1998 fortsatt utekontorer som ikke brukte systemet. Et annet problem var at Concorde var lite brukervennlig. Det ble derfor laget en egen brukermanual, men denne var så tunglest at de fleste ansatte på utekontorene ga opp å sette seg inn i den. Den største mangelen ved systemet var likevel at Concorde ble installert og brukt lokalt. Dermed kunne ikke informasjon som utekontorene (eller enheter i Norge – flyktningmottakene) registrerte i Concorde overføres elektronisk til administrasjonen

44 Eli Voksø, administrasjonssjef, intervju 05.12.05.
45 Strategi for informasjonsteknologi i Norsk Folkehjelp (1994), s. 2.

ved hovedkontoret i Oslo. Det innebar bl.a. at hovedkontoret ikke hadde full oversikt over økonomitilstanden på de ulike kontorene før revisjonsrapporten for det foregående regnskapsåret forelå (dvs. i slutten av april det påfølgende året). Verken den politiske eller administrative ledelsen fikk derfor god nok informasjon om tilstanden på hvert enkelt utekontor til å komme med korrigerende innspill. Dermed bidro ikke Concorde til å gi Norsk Folkehjelp det organisasjonen trengte: sterkere overordnet kontroll med det raskt ekspanderende aktivitetsnivået. Det var denne mangelen som regnskapstallene for året 2000 satte fingeren på. Følgelig mistet Concorde den siste rest av legitimitet og tillit i organisasjonen, og bordet lå dekket for nye e-forvaltningssatsninger.

2003-strategien som «Concorde-havariet» beredte grunnen for, reverserte tenkningen som IT-strategien fra 1994 baserte seg på. I det nye strategidokumentet ble det lagt vekt på at dagene til den fragmenterte IT-praksisen i Norsk Folkehjelp var talte. Isteden ble søkelyset rettet mot å samordne ressursbruken på IT-området og å sentralisere beslutningsmyndighet for å unngå at det vokste opp en ny flora av forskjelligartede programmer i ulike avdelinger og lokale enheter. Som i NLM, var derfor en mer helhetlig og effektiv administrasjonsordning hovedmålsetningen. Målsetningen skulle oppnås ved at all programvare ble lagret på servere ved hovedkontoret i Oslo, mens eksterne brukere – utekontorene, regionskontorene, flyktningmottakene, osv. – logget seg på serverne over ulike typer telesamband.[46] Dermed skulle kontrollen med hvilke programmer som var i bruk i ulike deler av organisasjonen sentraliseres på en langt sterkere måte enn tidligere.[47]

Få uker etter at IKT-strategien var blitt vedtatt, ble en handlingsplan for IT sanksjonert. For anskaffelse og implementering av en erstatning for Concorde, ble det spesifisert en investeringsramme på totalt 7 mill. kr., og i løpet av siste halvdel av 2003 ble ulike systemer og leverandører «målt og veid». Til slutt valgte Norsk Folkehjelp å satse på økonomi- og forvaltningssystemet Agresso Business World. Norsk Folkehjelp stilte to krav til den nye teknologien. For det første at mest mulig av økonomiske data måtte kunne legges inn i systemet og, for det andre, at det måtte være anledning til å ta ut mest mulig i form av analyser og rapporter. Når disse kravene var tilfredsstilt – et arbeid som foregikk i løpet av vinteren og våren 2004 – kunne selve implementeringen starte. Denne prosessen beskrives som en suksess. Det skyldes flere forhold, bl.a. at holdningen til innføringen av et nytt e-forvaltningssystem var positiv blant de ansatte, at Agresso-prosjektet var forankret i en IKT-strategi med klare målsetninger (og som raskt ble fulgt opp av en handlingsplan) og at ledelsen ved

46 Norsk Folkehjelp valgte derfor en tynnklient løsning basert på Citrix-plattform.
47 Se Styrende dokument for IT (vedtatt av Norsk Folkehjelps styre i januar 2003).

hovedkontoret stod bak prosjektet (med administrasjonssjefen som prosjektansvarlig). En annen avgjørende suksessfaktor, var avgjørelsen om å redusere antallet integrasjoner.

Den opprinnelige planen var at Agresso skulle integreres mot en rekke andre dataverktøy som var i bruk i Norsk Folkehjelp. Men integrasjoner innebærer at ulike programvarer må finjusteres i forhold til hverandre slik at data kan flyte fra den ene programvaren til den neste. Dette er tidkrevende, kostbart, komplisert og risikofylt arbeid: små feil kan få store negative konsekvenser. Dessuten må integrasjonene foretas på nytt hver gang oppdaterte versjoner av den eksisterende programvaren installeres. Derfor bestemte de ansvarlige for implementeringsprosessen seg for å redusere antallet integrasjoner fra 12 til 2. Ifølge den nye planen, skulle Agresso integreres mot medlems- og giverdatabasen (MySoft) og saks- og arkivsystemet (Acos).[48] Med denne beslutningen på plass, kunne arbeidet forseres: alle utekontorene installerte Agresso i løpet av sommeren og høsten 2004, og ved hovedkontoret gikk man over fra Concorde til Agresso sommeren 2005.

Styringsmuligheter og kulturendring

Implementeringen av Agresso hevdes å ha styrket ledelsens muligheter til å holde seg informert om og styre økonomiutviklingen innenfor de mange bistands- og mineryddingsprosjektene:

> *«Oslo har nå oversikt over budsjettene og pengebruken ute (…) Nå sendes det ikke ut like mange generelle rundskriv som tidligere. Masingen er blitt mer konkret og målrettet fordi Agresso gir mer informasjon til Oslo om tilstanden på hvert enkelt utekontor.»*[49]
>
> *«Nå er det laget strenge sentrale retningslinjer for budsjettering, rapportering, regnskapsføring, logistikk og innkjøp. Fra Oslo kan vi se om disse følges eller ikke.»*[50]

Sammen med det nye e-forvaltningssystemet er det altså laget andre og strengere rutiner for det administrative arbeidet: Agresso har lagt grunnlaget for

48 Per Ranestad, leder for Agresso-prosjektet, intervju 18.11.05.
49 Per Ranestad, leder for Agresso-prosjektet, intervju 02.12.05.
50 Eli Voksø, administrasjonssjef, intervju 05.12.05.

sterkere byråkratisering av administrasjonsarbeidet.[51] Det er kombinasjonen av disse tiltakene – teknologiske og byråkratiske – som Norsk Folkehjelp håper vil gi ledelsen større muligheter til å styre den profesjonaliserte virksomheten på en mer hensiktsmessig måte enn tidligere. Dermed skal det bli mulig å forankre det profesjonaliserte arbeidet sterkere i forhold til landsmøte- og styrevedtatte målsetninger: e-forvaltning skal sette Norsk Folkehjelp bedre i stand til å kontrollere at de ansatte (særlig i utlandet) bidrar til å realisere organisasjonens medlemsbestemte prioriteringer. Dette er spesielt viktig etter som den profesjonaliserte virksomheten er svært omfattende sammenliknet med størrelsen på medlemsmassen. Uten kapasitetsforbedringer på forvaltningssiden har det derfor vært en reell mulighet for at det profesjonelle og operative arbeidet frikoblet seg fra medlemsmassens ønsker og interesser. Om denne muligheten etter hvert kan elimineres, avhenger ikke bare av nye teknologisystemer og matchende administrative rutiner. Det dreier seg også om å gjennomføre en liten «kulturrevolusjon».

Her handler det om å endre det som beskrives som Norsk Folkehjelps «kollektive lederstil». På 1980- og 1990-tallet (og sannsynligvis tidligere også) ble det ansett som ønskelig og hensiktsmessig at alle ansatte kunne være med å påvirke Norsk Folkehjelps prioriteringer. Det skyldes at antallet ansatte var lite og at ekstensiv involvering i interne beslutningsprosesser ble oppfattet som en god måte å utnytte organisasjonens kompetanse og erfaringer på. Men etter at Norsk Folkehjelp vokste kraftig utover på 1990-tallet, ble den «kollektive lederstilen» lite effektiv, samtidig som den truet med å overføre for mye makt fra medlemsmassen til de administrative og operative delene av organisasjonen. Og etter innføringen av Agresso ble det klart at systemets styringspotensial ikke kunne utnyttes så lenge den «kollektive lederstilen» fortsatte. Det var istedenfor behov for tydeligere myndighets- og ansvarsfordelingen mellom den valgte ledelsen og de ansatte. Denne nyordningen av styringsstrukturen innebærer to ting. For det første at Norsk Folkehjelps nasjonale styre tar et fastere grep om den overordnede utviklingen av organisasjonsvirksomheten; for det andre at de ansatte (både i Norge og utlandet) blir mer fokusert på å etterleve rutiner, regler og beslutninger som den valgte ledelsen fatter. Med Agresso på plass kan de teknologiske forutsetningene for å få dette til være til stede.

51 Et eksempel på dette er praksisen med å skrive såkalte QMS-er. QMS (Quality Management System) er et system for rutinebeskrivelser som de ansatte har tilgang til via Norsk Folkehjelps intranett. Rutinebeskrivelsene oppfattes av mange ansatte som en unødvendig byråkratisk og kjedelig øvelse som de ikke helt ser poenget med. I 2006 fantes det bl.a. rutinebeskrivelser for bestilling av pizza, smørbrød og kaffe fra eksterne leverandører.

E-forvaltning i NLM og Norsk Folkehjelp

Analysen ovenfor har vist at NLM har lagt vekt på sentralisering og profesjonalisering av teknologi- og økonomi/regnskapsfunksjoner (gjennom opprettelsen av tvillingselskapene NLM IKT Service og NLM Økonomiservice). Også i Norsk Folkehjelp har man sentralisert ansvaret for teknologivalg til hovedkontoret. Men i motsetning til i NLM har ikke Norsk Folkehjelp valgt å overføre økonomi- og regnskapsarbeidet fra lokale enheter til hovedkontoret. Isteden har det nye e-forvaltningssystemet ført til sentralisering av styrings- og kontrollfunksjoner: økonomi- og regnskapsarbeidet utføres lokalt, men hovedkontoret kan titte de lokale enhetene (med unntak av lokalforeningene) i kortene på en helt annen måte enn tidligere. Dette kan bidra til å styrke den nasjonale og valgte ledelsens muligheter til å styre det profesjonaliserte og operative arbeidet. I NLM har slike styringsambisjoner vært noe mindre fremtredende. En viktig årsak til dette er trolig lekmannsideologiens vektlegging av lokale selvstendighet. Men samtidig har sentraliseringsambisjonene vært større i NLM (gjennom opprettelsen av NLM IKT Service og NLM Økonomiservice). Derfor har e-forvaltningstiltakene blitt møtt med større skepsis enn i Norsk Folkehjelp.

E-forvaltningstiltakene er i stor grad resultat av eksternt press, først og fremst som følge av organisasjonenes nære relasjoner til staten. Både NLM og Norsk Folkehjelp er derfor sensitive for endringer i de statlige rammebetingelsene, men tiltakene har også en viss forankring i interne behov – stagnasjonsproblemer i NLM og vekstutfordringer i Norsk Folkehjelp. Nye lovkrav til økonomistyring og regnskapsføring har derfor gitt startskuddet til tekniske, administrative og organisatoriske endringsprosesser som har til hensikt å gjøre organisasjonene (a) mer «administrasjons- og styringsvennlige» og (b) samordne og effektivisere prioriteringer og ressursbruk. Dermed legger staten (men også andre finansielle bidragsytere) sterke føringer på omstillings- og teknologiarbeidet. I begge organisasjonene oppleves eksterne krav til styring, kontroll og rapportering som byråkratiserende, dvs. at terskelen for hva som forventes av administrativ profesjonalisme øker. Samtidig synes e-forvaltningstiltakene i seg selv å føre til nye former for byråkratisering – flere rutiner og retningslinjer og nye kompetansekrav.

Organisasjonsendring, ny teknologi og statlige rammebetingelser

Hvis vi ser på konsekvensene av e-forvaltningstiltakene i NLM og Norsk Folkehjelp, avtegner det seg et relativt likeartet omstillingsmønster som til dels er kjent fra den øvrige frivillighetslitteraturen i Norge. Dette mønstret kan oppsummeres i følgende hovedpunkter:

- Statsavhengighet: Initiering av e-forvaltningstiltak skyldes i særlig grad nye lovpålagte krav fra offentlige myndigheter. Regelen virker å være at jo nærmere koblingen til staten er, desto sterkere slår nye krav til systemutvikling, administrativ profesjonalisering og hierarkisk styring inn i organisasjonene.
- Sentralisering: Nye e-forvaltningssystemer fører til at organisasjonene blir mer topptunge. Det skyldes at teknologisystemene administreres sentralt og at informasjon som tidligere lå skjult på lavere nivåer lettere kan leses, kontrolleres og benyttes av sentralt ansatte og overordnede organer. Samtidig er det en tendens til at administrasjonsoppgaver (spesielt relatert til økonomistyring og regnskapsføring) overføres fra lokale enheter til hovedkontoret.
- Profesjonalisering: Administrasjonsoppgaver overføres til ansatte ved hovedkontoret bl.a. fordi utførelsen av dem er mer kompetanseintensiv enn tidligere. Bruken av digital teknologi for å sentralisere økonomiske og administrative oppgaver er derfor (til en viss grad) et svar på behovet for å forankre arbeidet i større ekspertmiljøer.
- Byråkratisering: Behovet for at økonomiske og administrative oppgaver løses av eksperter ved hovedkontorene skyldes at oppgavene er blitt langt mer kompliserte og regelstyrte enn tidligere. Samtidig fører bruken av nye e-forvaltningssystemer til introduksjon av nye strategier, handlingsplaner, rutiner og retningslinjer.

I forhold til denne oppsummeringen (og fremstillingen ovenfor), er det flere ting som er verdt å merke seg. For det første at endrede statlige rammebetingelser (relativt nye og lovpålagte krav til økonomistyring og regnskapsføring) er den viktigste enkeltårsaken til at organisasjonene har gjennomført store utviklings- og e-forvaltningstiltak. Samtidig kan det synes som om kontroll- og rapporteringskravene som lovverket målbærer, representere en ny måte å regulere frivillige organisasjoner på (bl.a. ved at økonomistyringskrav og regnskapsføringsregler som tidligere bare omfattet privat næringsvirksomhet nå også inkluderer frivillige organisasjoner). Dette kan sies å være uttrykk for den nye styringsfilosofien (New Public Management) som har preget offentlig forvaltning i løpet av de siste 20 årene, dvs. villigheten til å importere styringsteknikker fra privat sektor.[52] Denne endringen i styringsfilosofi (og tilhørende teknikker) virker å innebære en forestilling om at frivillige organisasjoner i mindre grad enn tidligere målbærer verdier og interesser som har egenverdi i

52 For analyser av endringer i styringsfilosofi og teknikker i offentlig sektor, se for eksempel Lægreid og Christensen 2001 eller Tranøy og Østerud 2001.

kraft av sin folkelige forankring. Isteden fremstår organisasjonene (i relasjon til lovverket) som forvaltere av ressurser som kan være avgjørende for implementeringen av offentlig politikk. Derfor kan det synes som om de reguleres på måter som forsøker å sikre «bedre resultater for pengene».

Men endrede statlige rammebetingelser er likevel ikke den eneste årsaken til e-forvaltningstiltak. I tillegg spiller organisasjonsinterne utfordringer inn, enten det dreier seg om langvarige og problematiske utviklingstrekk (slik som i NLM) eller utfordringer knyttet til rask og omfattende vekst (slik som i Norsk Folkehjelp). Vi kan derfor si at statlige krav og forventninger til en viss grad fungerer som insitamenter for å iverksette reformer som organisasjonene uansett ville hatt behov for, men som gjennomføres raskere og blir mer omfattende enn hva de ellers ville vært.

For det andre finnes det en «skjult» faktor som påvirker utviklingsarbeidet i NLM og Norsk Folkehjelp: teknologisk endring. Teknologisk endring innebærer at nye systemer for administrativ databehandling er oppbygd på en slik måte at de legger til rette for sterkere sentral styring og kontroll (bl.a. ved at dataprogrammer som brukes lokalt ligger på servere ved hovedkontorene, mens aksess skjer via Internettet eller andre typer telesamband). Det er derfor et samspill mellom utviklingen av avanserte datasystemløsninger og statlige krav til administrativ profesjonalisering: kravene ville trolig ikke vært mulig å imøtekomme (og dermed lite hensiktsmessig å stille) uten at teknologien for å implementere dem er kommersielt tilgjengelig.

For det tredje at endrede statlige rammebetingelser – og den måten de implementeres på (via e-forvaltningstiltak) – representerer store og viktige omleggginger i forhold til organisasjonenes tradisjonelle oppbygning og virkemåte. Det viktige her er at de delene av organisasjonene som administrerer eller utfører profesjonalisert innsats – hovedkontoret, krets- eller regionskontorene og operative enheter (utekontorer, flyktningmottak, skoler, barnehager, leirsteder, osv.) – forsøkes sydd sammen (ved hjelp av avanserte datasystemløsninger) til «ett administrativt rike». Systemer, rutiner og retningslinjer for det tekniske og administrative arbeidet blir derfor i økende grad standardisert på tvers av enheter og organisasjonsnivåer (slik som i relasjon til bruken av Agresso i Norsk Folkehjelp), eller arbeidet overføres til sentrale forvaltningsenheter (slik som NLM IKT Service A/S og NLM Økonomiservice A/S). Det betyr ikke at for eksempel krets- eller regionskontorenes juridiske status endres, men at deres selvstendighet innsnevres: hovedkontoret blir nå den sentrale beslutningsenheten med hensyn til valg av tekniske og administrative løsninger.

I NLM har vi sett at denne omleggingen er møtt med skepsis og kritikk, fordi den rører ved organisasjonens tradisjonelle demokratisyn som springer ut av lekmannsideologiens selvstendighetstenkning. I Norsk Folkehjelp har ikke

«selvstendighetslinjen» stått like sterkt, men det gjenstår likevel å se om omlegging av organisasjonens «kollektive lederstil» (som trolig er nødvendig for at Agresso-systemet skal kunne brukes som forutsatt) lar seg gjennomføre. Det er også verdt å merke seg at lokalforeningenes relasjoner til sentralnivået ikke endres som følge av e-forvaltningstiltakene. De skal nyte den samme selvstendigheten som tidligere fordi organisasjonene ser dette som nødvendig for at virksomheten fortsatt skal kunne tuftes på et bredt og frivillig engasjement.

For det fjerde innebærer målsetningen om å samle den profesjonaliserte delen av organisasjonsvirksomheten til «ett administrative rike» at e-forvaltningstiltakene fremstår som relativt kompliserte teknisk-organisatoriske utviklingsprosjekter. Det skyldes at kostbare tekniske systemer introduseres samtidig med at etablert organisasjonspraksis endres. Spesielt tydelig er dette i NLM hvor ekspertintensive administrasjonskrav blir forsøkt ivaretatt ved å utvikle egne teknologi- og økonomimiljøer på sentralt nivå. Men også i Norsk Folkehjelp øker behovet for spesialisert teknisk og økonomisk ekspertise. Organisasjonen har derfor benyttet Agresso til å overføre regnskapsføringen fra enkelte operative enheter (flyktningmottakene i Norge) til administrasjonsavdelingen ved hovedkontoret, og har planer om å gjøre hovedkontoret til en økonomisk-administrativ rådgivningsenhet i forhold til kontorene i utlandet.

Hva betyr dette for organisasjonenes muligheter til å påvirke offentlig politikkutforming med bakgrunn i medlemmenes ønsker og interesser? På den ene siden kan det argumenteres for at påvirkningskraften svekkes: e-forvaltningstiltak signaliserer at datasystemløsninger, administrasjon og økonomistyring fremfor politikk og ideologi opptar organisasjonene. Det betyr samtidig at måten staten regulerer organisasjonene på får forholdsvis store konsekvenser for interne prioriteringer: penger må avsettes til teknisk-administrativ egenutvikling fremfor å brukes til andre formål. I tillegg har staten (og ikke-statlige

donorer) inntatt en mer aktivistisk og kritisk holdning til organisasjonene. I NLM merkes dette bl.a. gjennom usikkerheten som er skapt omkring finansieringen av friskoler (jfr. debatten om religiøse «ekstremskoler»[53]); i Norsk Folkehjelp ved at det har blitt vanskeligere å få statlig finansiering til prosjekter som uttrykker organisasjonens selvvalgte og medlemsbestemte målsetninger. Med basis i erfaringene fra NLM og Norsk Folkehjelp, kan det derfor synes som om innflytelse og påvirkning i relasjonen mellom stat og frivillig sektor er blitt mer ensrettet enn for 10 eller 15 år siden: staten legger ikke bare premissene for det interne utviklingsarbeidet, men stiller også flere krav til prosjektgjennomføring og resultatoppnåelse.[54] Det kan følgelig synes som om NLM og Norsk Folkehjelp både har gjort seg selv til og i større grad blir behandlet som det offentlige forvaltningsapparatets «forlengede arm».

På den annen side synes ikke ideologi- og verdifokuset i NLM og Norsk Folkehjelp å svekkes selv om utviklingsarbeidet og e-forvaltningstiltak legger beslag på store ressurser. Men ledelsen i begge organisasjonene uttrykker likevel at arbeidet er blitt mer «forvaltningspreget» enn tidligere, og at dette på sikt kan føre til at organisasjonene verdsetter kompetanse høyere enn verdimessig og ideologisk engasjement. Samtidig innrømmes det at mer «forvaltningspreg» har vært nødvendig, både for å få oversikt over og utnytte ressursene bedre og for å sikre at det profesjonaliserte arbeidet ikke «immuniseres» mot overordnet politisk styring. Det oppfattes derfor som en fordel at det profesjonaliserte arbeidet omgis av et strammere administrativt rammeverk enn tidligere. Håpet er at e-forvaltningstiltakene skal bidra til at de to organisasjonene settes bedre i stand til å kombinere forvaltningen av (a) store ressurser og kompetanse, (b) mange medarbeidere og (c) et stort aktivitetsmangfold med (d) medlemsbasert innflytelse og styring. For uten bedre kontroll med den profesjonaliserte virksomheten, er det vanskelig å se for seg at de ansatte ikke skal overta rollen

53 NLM mener at organisasjonens restriktive syn på homofili, samboerskap og gjengifte har gjort den til «skyteskive» for enkelte rikspolitikere og statlige institusjoner. For eksempel valgte NRK i 2005 å bryte samarbeidet med NLM-eide Mediehøyskolen på Gimlekollen da innholdet i høyskolens verdidokument (som bl.a. uttrykker organisasjonens syn på ulike typer samlivsformer) ble gjort kjent i Fædrelandsvennen.

54 Ny statlig politikk har også påvirket Norsk Folkehjelps inntektsgrunnlag. Frem til den statlige monopoliseringen av spillautomatmarkedet, hadde Norsk Folkehjelp i overkant av 30 mill. kr. i årlige inntekter fra denne virksomheten. Men da det i 2006 ble endelig klart at disse inntektene ville bli betydelig redusert, måtte organisasjonen iverksette en ny nedbemanningsprosess. Den endte med at hovedkontoret ble redusert med 10 stillinger. Stasningen på alternative inntektskilder, spesielt sponsing fra næringslivet, har derfor økt. Men det stiller Norsk Folkehjelp overfor nye krav til utvikling og innsalg av prosjekter, og til rapportering, dokumentasjon og donorpleie. Kostnadene knyttet til å generere og administrere penger er m.a.o. stigende.

som den dominerende kraften internt. Særlig viktig er dette etter som medlemmenes finansieringsrolle i NLM og Norsk Folkehjelp er svekket i løpet av de siste 25–30 årene, og at de ansatte har fått en mer fremskutt posisjon som i inntektsarbeidet. Det kan bety at medlemsbasert påvirkning, både i forhold til organisasjonens sentrale organer og overfor offentlige myndigheter, kan få trangere vilkår enn tidligere. Derfor kan det vise seg at e-forvaltningstiltak, ved å bidra til større administrativ profesjonalisering, også kan bidra til å styrke organisasjonenes demokratiske styringskjede.

Litteraturliste

Burt, Eleanor og John Taylor (2007): Voluntary Organizations in the Democratic Polity: Examining Web-Enabled 'Public Spaces'.» I J.E.J. Prins (red.): *Designing E-Government*. Alphen am den Rijn: Kluwer Law International.

Christensen, Tom og Per Lægreid (red.) (2001): *New Public Management. The Transformation of Ideas and Practice*. Aldershot: Ashgate.

Dunleavy, Patrick, Helen Margetts, Simon Bastow og Jane Tinkler (2005): «New Public Management is Dead – Long Live Digital-Era Governance.» I *Journal of Public Administration Research and Theory*, 16: 467–494.

Edwards, Arthur (2005): «Niches for New Intermediaries: Toward an Evolutionary View of Digital Democracy.» I Victor Bekkers og Vincent Homburg (red.): *The Information Ecology of E-Government*. Amsterdam: IOS Press.

Hill, Kevin A. og John E. Hughes (red.): *Cyberpolitics. Citizen Activism in the Age of the Internet*. Lanham: Rowman & Littlefield.

King, J.L. og K.L. Kraemer (1998): «Information Technology in the Establishment and Maintenance of Civil Society.» I I.Th.M. Snellen og W.B.H.J. Van de Donk (red.): *Public Administration in an Information Age*. Amsterdam: IOS Press.

Löfgren, Karl (2000): «Danish Political Parties and New Technology. Interactive Parties or New Shop Windows?» I Jens Hoff, Ivan Horrocks og Pieter Tops (red.): *Democratic Governance and New Technology*. London: Routledge.

Malina, Anna (1999): «Perspectives on Citizen Democratisation and Alienation in the Virtual Public Sphere.» I Barry N. Hague og Brian D. Loader (red.): *Digital Democracy. Discourse and Decision-Making in the Information Age*. London: Routledge.

Nilsen, Marte (2006): «ATTAC: For global rettferdighet.» I Magnus E. Marsdal (red.): *Økonomisk apartheid. Nyliberalismens verdensorden*. Oslo: Solidaritet forlag.

Pedersen, Karina og Jo Saglie (2005): «New Technology in Ageing Parties. Internet Use in Danish and Norwegian Parties.» I *Party Politics*, 11 (3): 359–377.

Putnam, Robert D. (2000): *Bowling Alone. The Collapse and Revival of American Community*. New York: Simon & Schuster.

Ranerup, Agneta (2001): «Elektroniska mötsplatser för kommunal debatt». I Åke Grönlund og Agneta Ranerup (red.): *Elektronisk förvaltning, elektronisk demokrati. Visioner, verklighet, vidareutveckling*. Lund: Studentlitteratur.

Schalken, Kees (2000): «Virtual Communities: New Public Spheres on the Internet.» I Jens Hoff, Ivan Horrocks og Pieter Tops (red.): *Democratic Governance and New Technology*. London: Routledge.

Schalken, C.A.T. og P.W. Tops (1995): «Democracy and Virtual Communities. An Empirical Exploration of the Amsterdam Digital City.» I W.B.H.J van de Donk, I.Th.M. Snellen og P.W. Tops (red.): *Orwell in Athens. A Perspectice on Informatization and Democracy*. Amsterdam: IOS Press.

Selle, Per og Bjarne Øymyr (1995): *Frivillig organisering og demokrati. Det frivillige organisasjonssamfunnet endrar seg 1940–1990*. Oslo: Samlaget.

Sivesind, Karl Henrik et al. (2002): *The Voluntary Sector in Norway. Composition, Changes and Causes*. Oslo: Institutt for samfunnsforskning.

Skocpol, Theda (2003): *Diminished Democracy. From Membership to Management in American Civic Life*. Norman, Okla.: University of Oklahoma Press.

Strandberg, Kim (2006): *Parties, Candidates and Citizens Online. Studies of Politics on the Internet*. Åbo: Åbo Akademi.

Sunstein, Cass (2001): *republic.com*. Princeton: Princeton University Press.

Tranvik, Tommy (2003): «Surfing for Online Connectedness: Is the Internet Helping to End Civic Engagement?» I Sanjeev Prakash og Per Selle (red.): *Investigating Social Capital. Comparative Perspectives on Civil Society, Participation and Governance*. New Delhi: Sage Publications.

Tranvik, Tommy og Per Selle (2007): *Digital teknologi i sivilsamfunnet. Omstillingsprosesser i fire frivillige organisasjoner* (kommer).

Tranvik, Tommy og Per Selle (2007): «The Rise and Fall of Popular Mass-Movements. Organisational Change and Globalisation – the Norwegian Case.» I *Acta Sociologica*, vol. 50, nr. 1: 57–70.

Tranvik, Tommy og Per Selle (2003): *Farvel til folkestyre? Staten og de nye nettverkene*. Oslo: Gyldendal Akademiske.

Tranøy, Bent S. og Øyvind Østerud (red.) (2003): *Den fragmenterte staten. Reformer, makt og styring*. Oslo: Gyldendal Akademiske.

Tsagarousianou, Roza, Damian Tambini og Cathy Bryan (red.): *Cyberdemocracy: Technology, Cities and Civic Networks*. London: Routledge.

Van de Donk, Wim; Brian D. Loader, Paul G. Nixon og Dieter Rucht (red.): *Cyberprotest. New Media, Citizens and Social Movements*. London: Routeledge.

Van de Donk, Wim og Bram Foederer (2001): «E-Movements or Emotions? ICTs and Social Movements. Some Preliminary Observations.» I J.E.J. Prins (red.): *Designing E-Government. On the Crossroads of Technological Innovation and Institutional Change*. The Hague: Kluwer Law International.

Wollebæk, Dag og Per Selle (2002): *Det nye organisasjonssamfunnet. Demokrati i omforming*. Bergen: Fagbokforlaget.

Wollebæk, Dag, Per Selle og Håkon Lorentzen (2000): *Frivillig innsats*. Bergen: Fagbokforlaget.

MAKING SENSE OF DIGITAL CASH

Maryke Silalahi Nuth

The Internet, which has grown vastly in size since the introduction of the World Wide Web, provides customers with additional venue for purchasing goods. One of the most revolutionary products developed in financial circles to facilitate Internet trade has been digital cash product. Although efforts to invent, introduce and implement digital cash systems have long been attempted and some people have envisioned digital cash to change and greatly affect international finance, the reality to date is that the impact of digital cash has been trivial. Many people are still not familiar with the concept of digital cash and there is even an open question what digital cash is. This paper elaborates concept and issues of digital cash (including legal issue) to give an overview on digital cash system and while doing so, perhaps offers explanation for the slow embrace of digital cash system by the market.

1. Nature

In essence, digital cash is digital representation of money or more accurately digital representation of currency.[1] There are many systems that can produce digital representation of money or currency. Different system assigns different name to their product despite the fact that they are essentially the same. Electronic money, computer money, virtual cash, cyber cash, internet cash, etc are just few examples. Therefore it is not surprising if no single term describing digital cash is widely known or more dominant than others.

A major change introduced in digital cash system concerns with the nature of money. Originally money was a physical substance like gold, silver or valued banknotes or coins but now it has become intangible exists as entries in bank records or as just digits stored in either chip of a smart card or on a customer's computer. A digitally signed payment message basically represents electronic transfer of money. Money can be transferred electronically because money is digits. Money is on-off switches. Money is a number in a computer or in a card. A bank account is a number in a bank's computer. Money is organised

1 It must be noted that the words money and currency, although used interchangeably and often synonymously, do in fact mean different things. Money is simply a means of communicating value, while currency is the physical manifestation of money. Currency gives money visible form.

transactional information. Money can be communicated by «wire», modem, co-axial or fibre optic cable, satellite or by modulated radio frequency, because it is digital data.

Like conventional bank cards digital cash is mainly designed as a substitute for ordinary cash. In addition, there are two major and distinct levels in which digital cash systems are expected to operate.[2] Firstly is to replace credit or debit card transactions with the transfer of *actual* digital value. This value derives from deposit of cash or transfer from a credit card, but such value then exists electronically in the hands of the customer. This «digitised» cash could then be used for the same range of purchases that have been historically handled by credit cards and ATM debits. Secondly, some digital cash systems are developed to handle smaller range of payments or micropayments. These products utilize simplicity and small economic scale to payment and transfers of much smaller amount of money feasible. There has been a talk about building a system that can handle micropayment as small as a tenth of a cent for some years. Nevertheless, the current systems focus on one cent to a few dollars as the range of transaction sizes.

2. Different Systems

There are many models of digital cash systems. Some of them are based on payment mechanism which are commonly used in everyday trade and thus are easily recognisable. The following are some of those models. It should be noted this is not an attempt to make (exhaustive) classification of existing digital cash systems. Such work requires more thorough and deeper research due to vast number of digital cash systems in the market and not to mention those under development.

Based on temporal relationship between cash withdrawal and receipt of the goods or service, there are generally three possible models of digital cash system: pre-paid, pay now and pay later: [3]

In ***pre-paid*** systems, ordinary money is withdrawn now, but the goods or service is actually purchased and received later. The card thus represents stored value, and is often referred to as a «stored value» card similar to prepaid phone cards. A generalised instrument of this type is «electronic purse» whose value may be spent on a variety of goods or services. Values stored in electronic

2 Froomkin, A.M., Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases, 15 U. Pittsburgh Journal of Law and Commerce 395 (1996).

3 J. Orlin Grabbe, Concepts in Digital Cash, Digital Finance: Index to Articles, 2000, 6 Feb 2007.

purse function very much like values stored in traveller's check. Most digital cash systems are prepaid. A successful example will be Mondex card.

In ***pay-now*** systems, payment is made at the same time as the product is received. This is similar to a situation when a person uses an ATM or other debit card to purchase gas at petrol station. Pay-now systems are often online, meaning they take place by making a connection to a central server or computer. Many of existing banking payment system can easily be modified to become pay-now based digital cash system while at the same time protecting privacy in which customer payment and receipt of goods as well as merchant deposit can take place simultaneously.

Finally, there are ***pay-later*** systems, an example of which occurs when one pays for dinner with a credit card. The seller (restaurant) will receive payment prior to the buyer's account being debited, because the card-issuer extends credit to the buyer in the interim. No noteworthy pay-later digital cash systems are in operation. However, credit may be easily introduced into a digital cash system by letting customers pay for digital cash with credit cards or by allowing large amount of value stored as digital cash for which there has not been any prepayment. This mechanism would appear to eliminate the possibility of anonymity in transactions because the transaction amounts would need to be collected and later presented for deduction from the spender's account.

Each type of digital cash has two varieties: online digital cash and offline digital cash depending on whether or not a third party (usually a bank or electronic money institution) needs to be involved in conducting a transaction.

Online systems involve authentication and authorisation server (a specialised dial-up digital cash or VISA computer, for example). Information provided by customer is compared against information in a central database. Transaction between buyer and seller (customer and merchant) will not take place unless a third party server firstly verifies buyer's identity (in non-anonymous digital cash systems) or validity of buyer's digital cash (in both anonymous and non-anonymous systems) and authorises payment to the seller. Digital cash systems that are purely software-based are usually online.

By contrast, there is no third party involvement in the payment process using ***off-line systems***. This model has no need for immediate communication with a third party such in the online systems. However, this model requires additional tamper-resistant hardware (for example in form of PCMCIA or smart card) and a more sophisticated cryptological protocol.

Value can be stored in various ways in off-line systems but most commonly is by using devices that are variously called stored-value cards, electronic purses or electronic wallets («Devices»). Money is stored in these Devices as

numbers just like balance in bank account book or bank's computer and can be spent in different manners depending on the system model:

- ***Balance-based system***, the Devices record a number and a currency designation in a numeric register for example: «Nok 100». Upon spending certain amount, the stored value will be reduced by this amount.
- ***Coin-based system*** in which each coin is identified by a set of numbers which constitute signature on the coin. These coins are digital information preserved in computer (and thus sometimes facilitate online system too) or smart card memory and each of them represents a given value. Thus, the total sum of coin value is equal total value stored in the Devices. A person can only spend his coins by transferring his signature to another person.[4] A payment of Nok 50 might involve the transfer of five coins each worth Nok 10 and bears individual signature.
- In ***Combine system*** the balance number is stored along with a series of uniquely identified transactions called «*electronic checks*». Unlike coin-based system, the size of each check in this system is not pre-determined; user can write down any amount he likes spending. To each electronic check is assigned a unique signature reflecting parties to the transaction and currency amount. The deposited value would be stored and compared against each electronic check withdrawal.

3. Characteristic

Since digital cash is actually meant to substitute physical currency, digital cash systems have been developed with the intention to have as close characteristics as possible with physical currency. Like real cash, it should be anonymous and reusable. This means, when digital cash is used to purchase something over the Internet, there is no way that such cash can be traced back to the buyer. It should also be possible to reuse the cash further or to circulate it from person to person with the same degree of anonymity. A true digital cash system should be able to accommodate these characteristics. Such characteristics are also in fact key differences between digital cash and bank (credit) card systems. Up to date there is no digital cash systems that have managed to fulfil these two characteristics.

Other characteristics of physical currency desirable for digital cash include indefinite and widely accepted. The last one is very crucial in making digital

4 The use of «blind signature» protocols allows transactional anonymity to be maintained even when a signature is transferred.

cash to be truly practical. In the framework of making their system more widely accepted and flexible, some digital cash systems developer also include portability and divisibility as their system characters. Portability means that digital cash can be transferable between different devices such as computers and smart cards. Divisibility means the system is not based on rigid predetermined currency amount and it should be possible to divide digital cash into smaller ones.

The above mentioned characteristics are important since they can help to explain why various interest groups advocate different designs of payment systems as well as consequences of the implementation or use of digital cash system on numbers of area.

3.1. System Security

Strong encryption techniques will help provide security for very sensitive information such as financial transactions on an insecure data transfer infrastructure like Internet or other public communication networks. Payments in digital cash system are usually done in form of encoded messages representing the encrypted equivalent of digitised money. Such financial transaction data are usually sent over the public communication networks. Cryptology provides methods of securing data and prevents unauthorized access to such data. Information that is hidden and signed by using cryptological protocol can be thought of as having been locked. Associated with this lock is an appropriate key and usually there are two keys, public and private key. To achieve secure data transfer, the encryption key is made public while the decryption key is kept private. In a data transfer, the sender first obtains the recipient's public encryption key and encrypts the data using this public key prior to sending it off. As such, only the intended recipient can successfully decode the message.

System security does not only concern security of data transfer but also security of the technology used in the system itself. Real digital cash system should be able to detect and prevent double spending problem i.e. where the system allows its user to make an indistinguishable copy of a piece of original digital cash and spend both copies. Avoiding double spending in online digital cash system is relatively easier when compared to offline digital cash system. Online digital cash systems usually require merchants to contact the issuing bank's computer on every sale to check with the bank's computer database of spent pieces of digital cash. If the bank computer confirms that the digital cash has already been spent, the merchant can refuse the sale. This mechanism is similar to credit card verification at the point of sale. On the other hand, detecting double spending in offline digital cash systems is more complex. In a

smart card based digital cash system, a tamper-proof chip called the 'observer' can be inserted in the card. This chip is basically a mini database containing information of all digital cash spent by that smart card. This chip will detect any attempt to copy some digital cash or to spend it twice, and would not allow the transaction. It is also not possible to erase data contained in this chip without permanently damaging the smart card, hence the term tamper-proof. Other offline digital cash systems prevent double spending by making it possible to identify the double spender by the time the digital cash is back in the bank system. The complete trails of digital cash can be accumulated and thus it is possible to detect where and when a particular digital cash lastly appeared as single piece. In other words, the bank can track when the digital cash was copied or spent more than once and accordingly identify the double spender through the transaction trails. It is reasoned that if people know that they will get caught when the digital cash is back in the bank system, they will think twice before making any double spending attempts and as such it will minimize double spending attempts. Of course, this would mean that digital cash system is not anonymous as the bank will have trails of the spent digital cash as well as its spenders.

3.2. Anonymity

One of the characteristics expected of digital cash which often considered as the main key for the success of digital cash is anonymity. A person who spends his electronic tokens does not need to reveal his or her identity to the merchant or to any third party. Of course in certain situations there may be a need to unravel the digital tokens to reveal the entity or person to who it was originally issued as in case of fraud or double spending attempts where the same piece of digital cash is presented twice for payment without the knowledge of the legal owner of the digital cash.

Anonymity generally means inability to determine individual spending patterns. Banks or other financial institutions, even when colluding with merchants, should not be able to link (*unlinkability*) or trace (*untraceability*) a person's transactions. Unlinkability refers to inability of the banks or other financial institutions to determine that two payments were made by the same customer. Untraceability refers to inability of the banks or other financial institution to match withdrawals of digital cash with subsequent payments. To have untraceability, the information that a person reveals about him by making payments must be statistically independent of the information he reveals when making withdrawals. Several levels of untraceability can be identified. It can be argued that complete untraceability only exists if no record what

so ever is generated during payment process. Since any electronic transaction invariably creates some data, only cash transactions yield this level of untraceability. In digital cash systems, untraceability can be achieved by designing the system in such way so that it is only the payer who can obtain transaction details directly. The protocol can also be designed so that no two payments can be linked to each other.

Up to now there is no digital cash system that is truly anonymous. At some point digital cash system will require third party involvement in the scheme. Most digital cash systems involve bank or other financial institution in the issuance of digital cash. A bank is integral to the scheme since it is required to hold collateral and to provide ultimate settlement of digital cash to more directly convertible currencies. This may yet prove to be a significant obstacle to the realisation of the scheme.

3.3. Universality

To be able to substitute physical currency, digital cash must be universal in its characteristics. Universality here refers to the possibility to use digital cash in many different places with relatively indefinite time. This means that digital cash must not have rigid limitation of its validity time or the places or merchants where it can be spent. To achieve this, digital cash needs also to be easily transferable not only between customers and merchants but also between customers themselves. Not many existing digital cash systems facilitate direct transfer between customers. Beside technological restrains, there are also money laundering and tax consideration behind this situation. If the customers are allowed to transfer big amount of money between themselves without involving bank or other financial institution, there will be no control on the transactions. As such, digital cash system will be very attractive not only to money launderers but also to tax evaders.

Re-useable digital cash, while facilitate universal use of digital cash as form of payment, can be a challenge to implement as it would require technological features that can differentiate legally re-used digital cash and illegitimate double spent digital cash.

3.4. Transaction Cost

Digital cash systems operate in low transaction costs. By cost here means the amount of money a customer is effectively charged for using the system for example for purchase of goods over the Internet. Transaction cost in digital cash systems can be reduced by eliminating the need for online clearance or by

cutting the hardware and communication expenses. This can be found especially in the pre-paid digital cash systems. Online clearance is waived as they are prepaid and often access verification is also waived because usually only small amount of money is at risk. This leads to very low financial transaction costs and accordingly fast transactions. While no reliable statistical information on the cost per transaction is available, it is estimated that the cost will be around $0.01-$0.05 per transaction, or even lower, as opposed to credit card transaction in the USA and Australia which respectively in the amount $1.20 and $A2.10.[5]

4. Notable Examples

Some of digital cash systems have been implemented for use. It is often that each system only has relatively small group of customers compared to the total size of Internet population. Therefore they become unattractive to potential Internet vendors and in turn, this keeps the numbers of customer down as very little can actually be bought using this system. This is not to say that none of digital cash system is technologically or commercially viable. In fact, the following digital cash systems are notable due to either its technology or its wide use.

DigiCash

DigiCash was one of the most known digital cash systems introduced in 1994. The system managed to effectively transmit electronic money using more than thirty participating merchants linked to the Internet. DigiCash suffered a setback in 1998 when the only U.S. bank offering its scheme, Mark Twain Bank, dropped the offering. DigiCash then closed its operations and liquidated its assets. Although no longer in operation, DigiCash technology is still in the market and up to date there are a number of major banks in Europe and Australia offer or are testing digital cash based on DigiCash technology.

Payments in DigiCash consist of uniquely coded digital tokens that are established in such a way as to prevent duplication or fraud. Under this scheme, bank customers would use local currency to buy an equivalent amount of digital cash from a bank. The system is based on single use token system. Customer generates blinded electronic coins and sends them to his bank to be signed with the bank's private key. Using the «blinding» technique, the bank

5 A. Furche and G. Wrightson, Computer Money, Dpunkt, Verl. Fur Digitale Technologie, 1996.

can validate the coins without knowing the customer's identity.[6] The bank signs the coins, deducts the amount from customer's account and sends the signed coins back to the customer. The customer then un-blinds them and further use them for a purchase at the shop. The shop verifies the authenticity of the coins using the bank's corresponding public key and sends the coins to the bank where they are checked against the master list of notes already spent. The amount is deposited into the shop's account, the deposited confirmed and the shop in turn sends out the goods. All communication over the network is protected by encryption. As a result, the customer can remain anonymous towards the shops, and the bank can not trace single transaction as it cannot correlate banknote numbers. In addition, every payment generates its own receipt in an encrypted form that only the customer can decrypt. By using the blinding technique, the customer prevents the bank from associating subsequently spent coins with withdrawals from his bank account. Therefore, the bank is unable to know when or where the customer shopped, or what they bought.

A person must open a bank account before he can get «E-Cash» to download and spend. This product is focused on large payments and the information given does not mention micropayments at all. As in many similar digital cash systems, customer must locate the merchant accepting DigiCash, generally through DigiCash's Web Page. Anonymity of the payor is promised although the payee must return the E-Cash to one of the host banks to recover the value.

Mondex

Mondex[7] is a stored value card system that has been in the market for some times and is still in use up to date. The system is operated by bank(s) which create, sell, and redeem the «electronically stored value» (ESV) on a memory chip on Mondex card. Such chip is often referred to as purse or wallet and is divided into five separate pockets, allowing up to five different currencies to be held on the card at any one time. ESV is thus just another form of money: dollars, if denominated in dollars; pounds, if denominated in pounds, and so on.

Mondex allows its customers to make online purchases without giving any personal details. The stored value behaves just like cash since it can be used in sale and purchase transactions as well as instant transfer of value between

6 Therefore, this prevents the bank from recognizing the banknotes as having come from the customer's account. The blinding technique is much used in other digital cash system such as in CyberCash and CyberCoin.

7 http://www.mondex.com

merchants and customers without any requirement of signature, PIN or transaction authorization.[8]

PayPal

Claiming to be the world's largest Internet-based payment system, PayPal[9] provides instant and secure online payment and money transfer over the Internet. PayPal also offers certain degree of anonymity to its user, although not totally. Indeed, PayPal users can make payment or money transfer without revealing their credit card number or other personal information to the merchants. But since PayPal system is account-based, to participate in the scheme users must firstly open an account in a real financial institution. Hence customer's record will be maintained in such financial institution.

Since its integration into eBay, PayPal has been more widely used in the world as more than 70 percent of all eBay sellers offer PayPal as payment option. PayPal has also been successful to expand beyond the eBay market. It is estimated that PayPal nowadays has more than 75 million individual and business users. Merchants participating in PayPal system usually set up a PayPal storefront on their payment process. To do payment, customers can choose to click on PayPal logo which will send them into a login page for PayPal account. There customers can transfer appropriate transaction amounts to the merchant. If a web site only accepts credit cards, PayPal can still be used to do the payment as long as the merchants accept MasterCard. Users can use the «PayPal Debit Bar» to get a virtual MasterCard number and the funds will be deducted from the PayPal account.

GlobeID

The GlobeID[10] payment prototype by GCTech is operated by the French Bank of Mars and enables customers to test secured and certified purchases from merchants over the Internet. GlobeID's technology offers a wide variety of payment methods, such as electronic purse, virtual electronic purse, micro-payments, magnetic stripe or chip based bank cards. Merchants license the virtual cash register from GlobeID, and customers get the Wallet Interface Module (WIM) for free to use on their computers. The WIM is an application/interface

8 Hence the chief function of the «stored value» is as a medium of exchange and not, as the name might imply, as inter-temporal savings which is the usual meaning of the phrase «store of value» in economic discussions.

9 http://www.paypal.com

10 http://www.globeid.com

that can govern a customer's digital cash and stored value accounts, though the information on these accounts (and any stored value) exist only on the GlobeID Operator's server. Customers can make purchases over the Internet and make a selection from their WIM which payment option they desire. Their information is verified by a merchant with the Operator and the identity of the buyer or other information remains invisible to the merchant. The GlobeID technology is already operational and integrated with major merchant servers, such as Microsoft Commerce Server. Via its licensees more than 30,000 customers have access to GlobeID payment system and hundreds of merchant kits have been distributed in Europe, Latin America and the Middle East.[11]

Since 1999 GlobeID has developed a wallet for customers to make payments from an ultra-thin device such as a wireless phone, TV set-top box or network computer. Cable TV and wireless phone service providers can use (and some of them have actually been using) this service to add payment functions to their network applications.[12] GlobeID has also developed payment systems for open smart-card devices such as the ePurse which can be plugged into the computer to make Internet purchases with smart cards as well as to buy items from vending machines such as subway or buss tickets. Such system has been widely deployed in Germany, the Netherlands and Belgium.

5. Legal Issues

Use of digital cash generally raises some questions about privacy, money laundering, and consumer protection.

5.1. Privacy

The effect of digital cash system on privacy depends on which system is used and, often, the details of how the system is implemented. Some digital cash systems have privacy-destroying effect whereas others can have a mixed effect on privacy. The major privacy-enhancing feature offered by any of digital cash systems as compared to traditional cash is that transactions under most schemes need not be face-to-face, a potentially significant privacy advantage. Nevertheless the relative anonymity achieved by dealing in cash is missing

11 UC Berkeley School of Information Management and System, Exploring Digital Cash: Wallets and Multiple Payment Products, available on http://www2.sims.berkeley.edu/courses/is204/f97/GroupE/wallets.html accessed 12 October 2007.

12 Georgie Raik-Allen, GlobeID Rakes in the Euros, RedHerring, The Business of Technology, 1 July 1999, available on http://www.redherring.com/Home/9013 accessed 12 October 2007.

because the level of privacy that can be provided is limited due to technical limitations. When customers use traceable payments mechanism to purchase goods or services, each payment creates the possibility of a record which, when combined with other similar records, becomes a detailed consumer profile. If, however, availability and ease of use of Internet commerce cause costumers to shift cash sales and credit card sales to digital cash system, the effect will be the increase of amount of information available on costumer's buying habits. Individual's financial transactions can present a cogent picture of most of his activities, relationships and even physical movements. An intruder gaining access to his payment dossier would be able to trace his habit, movements and attitude from the data.

Up to date there is no truly anonymous digital cash in existence. Truly anonymous digital cash would be possible if banks supporting digital cash system are willing to open anonymous accounts and to accept deposits in digital cash. When a bank account is anonymous, withdrawals and deposits cannot be traced to the account holder. In this scenario, anonymous bank accounts, combined with anonymous purchases and payment, would be even more private than cash, since both the seller and buyer could mask their identity.

5.2. Electronic Money Laundering

It should be noted that even if a bank wants to offer truly anonymous digital cash system, regulatory authorities would likely to oppose it. Untraceability of payments in digital cash system can be misused for criminal activities and money laundering. This what sometimes triggers the increase of electronic surveillance by governments or other authorised institutions engaged in computerised record-keeping and data mining, although tracing of person's spending is *prima facie* extremely intrusive on privacy.

Some offline stored-value cards are designed to also allow transfer of digital cash between customers. As such, it raises the greatest concern of money laundering. If there is no limit on the amount that can be loaded on a stored-value card, then the card can become a much more attractive means of moving black money. Smuggling a smart card loaded with one million kroner of value or transferring one million kroner worth of digital coin is certainly easier than smuggling a suitcase of cash. Nevertheless, given that until today participation in digital cash system including acquiring smart card based digital cash mostly requires entrance to regular banking system, it should still be possible to track movement of big money. Banking system has its own regulations with regards to transfer of money including reporting requirement on the transfer involving big amount of money. Indeed, money launderers may divide the transfer into

many small transfers below the monitoring threshold to avoid reporting obligation triggered by large transactions in currency. Fortunately, comprehensive anti money laundering regulations usually require bank or financial institution to report any unusual transactions in their customer's accounts for example repeated receipt of many small payments which when totalled form a big amount of money as often be the case in money laundering scheme. In other words, as long as digital cash transfers from and to particular countries pass through the banking system, the concerned digital cash system does not pose particularly serious money laundering threats. Nevertheless, it should be noted that its ease of use may tempt or encourage money laundering attempts.

5.3. Consumer protection

Some consumer protections issues can also be raised by the use of digital cash system. These include: What happens in case of lost cards? What happens in case of unauthorised transactions? What happens when a transaction goes wrong in some ways? How are costs and charges to be distributed among the players in digital cash system? Perhaps, some of these problems can be dealt with the existing consumer protection laws and regulations. Even so, the technical character of digital cash system may not necessarily be recognised in the existing regulations as illustrated in the case of lost of smart card. In one hand, this can be considered as the same with lost of physical currency and thus cardholder should bear the loss of the stored value. On the other hand, it is technically viable to program a *lock* into the card so that it cannot be used without a key. Should the issuer then be required to issue smart cards with lock? Should the liabilities be different where there is a possibility of locking the smart card?

The issues surrounding transaction security are no less interesting. Security concerns have frequently been limited to discussions about encryption while in fact it also concerns protection of consumer's rights. As consumers, users of digital cash system have the right to have their transaction not diverted, misidentified or otherwise misplaced. Consequently, digital cash system must be technically secured and functional. Such system must also be reliable in a sense that participating merchants will deliver what was paid for, that the merchant is real (not a fraudulent extraction scheme) and that redress exists for disputes if the product turns out to be unsatisfactory. All of these are within the sphere of consumer protection agenda.

6. Concluding Remarks

The foregoing demonstrates that although there are many attempts to develop digital cash systems, there is no true cash-like system. The existing digital cash systems, although strive to match physical currency, do not possess all characteristics of physical currency. Consequently, the role of digital cash is more like a viable alternative or supplement to, rather than replacement for, physical currency. Nevertheless, given that today there are lots of different ways of doing financial transactions (e.g. cash, checks, debit/credit, wiring money, traveller's checks, etc) and each with its particular point, we are still going to see that much diversity in digital cash and different digital cash systems will continuously be developed. The high fixed costs of credit card transactions as well as its electronic trails make them particularly unsuited for high-volume Internet sales. Therefore, there is still room in the market for yet other types of payment mechanisms. Digital cash systems that are safe, privacy enhancing and low cost will certainly be welcomed by customers as well as merchants.

MØTE MELLOM FORVALTNINGSRETTEN OG PERSONOPPLYSNINGSRETTEN*

Dag Wiese Schartum

1. Innledning

Den norske forvaltningsloven ble vedtatt i 1967. Bakgrunnen var en sterkt voksende offentlig forvaltning med utstrakt myndighet til å treffe vedtak vedrørende den enkelte borgers plikter og rettigheter. Motivasjonen var å «trygge den enkeltes rettsstilling».[1] Noen år etter at forvaltningsloven var vedtatt, ble en ny lovgivningsprosess initiert. Formålet var å «beskytte individet mot utilbørlige inngrep i integriteten» i tilknytning til «bruk av EDB ved opprettelse og drift av offentlige persondata system».[2] Begge lovgivningsarbeider var med andre ord motivert i ønsket om å beskytte den enkelte. Mens forvaltningsloven gjaldt beskyttelse av individets rettssikkerhet og rettsstilling generelt, gjaldt arbeidet med personvern spesielt beskyttelse av den enkeltes integritet, herunder ikke minst i forhold til offentlig forvaltning. På en måte kan en si at spørsmål om ivaretagelsen av rettssikkerhet delvis ble gjenstand for fortsatt diskusjon og regulering under betegnelsen personvern. Denne artikkelen tar utgangspunkt i denne parallellen.

I tidlig rettsteori i Norge vedrørende personvern stod det forvaltningsrettslige perspektivet sentralt. Personvern ble i stor grad diskutert i sammenhenger der personopplysninger inngikk i beslutninger om den enkelte. Det ble understreket at beslutningsgrunnlag skulle være saklig, og for øvrig ble det lagt betydelig vekt på aspekter knyttet til enkeltsaksbehandling; «På den måten kan vi se på personvern som en del av spørsmålet om fair saksbehandling.»[3] Etter hvert ble det utviklet en «interesseteori» der de viktigste elementene i

---

* Artikkelen er opprinnelig publisert i Schartum (red.) «Elektronisk forvaltning i Norden. Praksis, lovgivning og rettslige utfordringer» (Fagbokforlaget 2007). Boken inneholder både eksempler på konkrete systemløsninger fra de Nordiske landene og en rekke drøftelser av rettslige implikasjoner av IKT i offentlig forvaltning.

1 Til grunn for lovvedtaket lå det en grundig utredning, se Innstilling fra Komiteen til å utrede spørsmålet om mer betryggende former for offentlig forvaltning (Forvaltningskomiteen), oppnevnt 5. oktober 1951. Innstillingen ble avgitt 13. mars 1958.

2 Til grunn for lovvedtaket lå to offentlige utredninger. Sandvik-utvalget (NOU 1974: 22) utredet primært med utgangspunkt i privat sektor, mens Seip-utvalget (NOU 1975: 10, s 11 og 12) primært tok utgangspunkt offentlig sektor.

3 Blekeli 1976, s 23.

personvernet ble formulert. Stort sett var interessene formulert uavhengig av offentlig eller privat sektor, men «interessen i borgervennlig forvaltning» ble likevel løftet frem idet en gjorde oppmerksom på «faren for at forvaltningen skal miste sitt menneskelige ansikt».[4]

Mens forvaltningsloven klart ble avgrenset til «den virksomhet som drives av forvaltningsorganer» (§ 1), kom den norske loven om personregistre[5] og senere personvernlovgivning til å inneholde en felles regulering av personvern, uavhengig av sektor. Sammenhengen mellom rettsikkerhets- og personverngarantier ble imidlertid lite synlig i den norske lovgivningen og i de etterfølgende diskusjonene. Slik skjedde det at personvernet kom til å inneholde elementer med klar relevans for enkeltsaksbehandling i offentlig forvaltning, men uten at regelverkene viser til hverandre. I denne artikkelen er ambisjonen å tydeliggjøre noen vesentlige forbindelseslinjer mellom rettssikkerhet og personvern knyttet til enkeltsaksbehandling i dagens elektroniske forvaltningen.[6] Opplegget er å ta utgangspunkt i bestemmelser i forvaltningsloven og vise hvorledes personopplysningsloven får vesentlig innvirkning på den samlede rettsanvendelsen.

For den elektroniske forvaltningen er disse sammenhengene mellom forvaltningsloven og personopplysningsloven helt vesentlige. Forvaltningsloven har saksbehandlingsregler som direkte gjelder behandling av enkeltsaker og -vedtak. Bortsett fra særlige forskriftsbestemmelser vedrørende elektronisk kommunikasjon med og i forvaltningsorganer[7] og gjennomførte justeringer av lovteksten vedrørende krav til skriftlighet og underskrift,[8] er forvaltningsloven formulert uten tanke på IKT. Personopplysningsloven er som sådan formulert med tanke på at det skjer elektronisk behandling av personopplysninger. Den gjelder også for forvaltningens enkeltvedtak, og personopplysningsloven supplerer derfor forvaltningsloven på viktige punkter.

Forvaltningsloven bygger hovedsakelig på forutsetninger om at offentlig forvaltning gjennomfører manuell og individuell saksbehandling. Personopplysningsloven bygger på sin side hovedsakelig på forutsetninger om at enkeltpersoner og samfunnsinstitusjoner – inkludert forvaltningen – utfører automatisert behandling av personopplysninger, innen enkeltsaksbehandling og ellers. For forvaltningen representerer forvaltningsloven en vel kjent regule-

4 Selmer 1987, s 14, min understrekning.

5 Lov av 9. juni 1978 nr. 48 om personregistre mm (opphevet).

6 Parallelle problemstillinger gjelder også manuell saksbehandling, men dette kommer jeg ikke spesielt inn på i det følgende.

7 Forskrift av 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

8 Se ot.prp. 108 (2000-2001) om lov om endring av diverse lover for å fjerne hindringer for elektronisk kommunikasjon.

ring, og konfliktnivået i tilknytning til utformingen av elektronisk forvaltning er tilsynelatende lavt. Personopplysningsloven fremstår på den annen side som mer kontroversiell, der forvaltningen må forholde seg til en aktiv tilsynsmyndighet (Datatilsynet) med sterke meninger om hvorledes det er mulig å innrette forvaltningen. Ideelt sett burde de to regelsettene bli vurdert i sammenheng, og samlet sett fremstår de som mer enn summen av begge lover.

Gjennomgangen i denne artikkelen vil vise at disse to lovene ofte må fortolkes under ett, og at det derfor er uholdbart å se ivaretagelse av rettssikkerhet som noe adskilt fra personvern (og omvendt). Jeg går spesielt inn på forvaltningens utredningsplikt og forholdet til personopplysningslovens krav til opplysningskvalitet, samt bestemmelser om retting og sletting mv (avsnitt 2). Videre tar jeg opp spørsmål om taushetsplikt, og sammenholder disse med bestemmelser i personopplysningsloven om formålsbestemthet og informasjonssikkerhet (avsnitt 3). Også bestemmelser som vedrører innsyn og åpenhet blir sett i sammenheng i avsnitt 4. Til slutt ser jeg på sammenhengen mellom reguleringen av tilsynsmyndighet innen forvaltningsloven og personopplysningsloven, i det jeg særlig vurderer myndighetssituasjonen i tilknytning til utformingen av elektronisk forvaltning (avsnitt 5). I konklusjonen tar jeg opp spørsmål av regulatorisk karakter. Spørsmålet er hvorledes vi best kan innrette lovgivningen for å sikre at sammenhengen mellom regelsettene som skal sikre personvern og rettssikkerhet fremkommer på en helhetlig måte (avsnitt 6).

Artikkelen gjelder direkte norsk lovgivning. Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)[9] bygger imidlertid delvis på felles nordiske diskusjoner.[10] Lov om behandling av personopplysninger mv (personopplysningsloven), bygger på EUs personverndirektiv,[11] som alle de nordiske landene er bundet av og har implementert i sin nasjonale lovgivning. Selv om det er betydningsfulle forskjeller mellom lovgivningen i de ulike landene, er det derfor grunn til å tro at mange problemstillinger etter norsk rett vil ha paralleller i andre nordiske lands rett.

9 Lov av 10. februar 1967.

10 Som ledd i forarbeidet til forvaltningsloven ble rettssikkerhetsspørsmål bl.a. drøftet på det Nordiske Administrative møte i 1949, det Nordiske handelsmøte i 1950 og det 19. Nordiske Juristmøte i 1951.

11 Direktiv 95/46/EF.

2. Utredningsplikt i den elektroniske forvaltningen

2.1 Generelt om rettslig regulering av forvaltningsorganers saksutredning

I norsk forvaltningsrett har forvaltningsorganet et selvstendig ansvar for at saker blir riktig og tilstrekkelig opplyst («utredningsprinsippet»). Utredningsprinsippet innebærer imidlertid ikke at det er vedkommende forvaltningsorgan som skal treffe vedtak som må utføre saksforberedelsen selv. Prinsippet innebærer imidlertid at dette organet må sørge for at sakene blir opplyst på tilstrekkelig måte, for eksempel ved at de ser til at andre forvaltningsorganer, private virksomheter og/eller sakens parter skaffer til veie et tilstrekkelig beslutningsgrunnlag.[12] I den grad forvaltningen ønsker å pålegge private å inngi opplysninger til forvaltningsorganet, innebærer legalitetsprinsippet at slike pålegg ofte må ha hjemmel i lov. I mange tilfelle inneholder derfor lovgivningen bestemmelser om oppgaveplikt. Overfor parter i forvaltningssaker er det ofte bestemmelser som pålegger eller tillater den enkelte å initiere saksbehandling, samtidig som det er bestemt at dette skal skje ved det blir gitt slike opplysninger som forvaltningsorganet etterspør.[13]

Utredningsprinsippet kan etter dette sies å representere et temmelig fleksibelt utgangspunkt. Årsaken er forvaltningsmyndighetens adgang til å legge til rette for at andre enn forvaltningsorganet selv bidrar til å opplyse saken. Likevel utgjør legalitetsprinsippet en grense for hva slags utredningsoppgaver som kan pålegges de parter og andre aktørene uten at dette følger av loven. Her ligger en første utfordring ved utformingen av en elektronisk forvaltning: Når forvaltningen utvikler eller tilpasser nye systemløsninger med tilhørende saksbehandlingsrutiner, kan dette i for stor grad bli sett på som teknisk-praktiske valg uten at juridiske rammer iakttas. Spesielt i forhold til private parter og kommuner, kan endringer i saksutredning og informasjonsflyt innebære at en må gjennomføre endret regulering av oppgaveplikter, plikter til å bruke fastsatte Internett-baserte rutiner for innsamling av saksopplysninger fra parter mv.

Lovgiver kan fastsette oppgaveplikter, plikt for parter til å gjøre bruk av forvaltningens elektroniske rutiner for informasjonsinnsamling mv. Slik sett kan forvaltningen frigjøres fra arbeidsoppgaver som parter og ulike andre aktører (oppgavegivere) som har relevant informasjon kan overta. Lovvedtak innebærer imidlertid ikke at forvaltningsorganet blir ansvarsfri i forhold til de utredningsoppgaver som parter og andre skal løse. Et vesentlig poeng er at det

12 Forvaltningens utredningsplikt er inngående drøftet i Hans Petter Graver, Alminnelig forvaltningsrett, Universitetsforlaget 2002, s 403 – 412.

13 Se f.eks. folketrygdloven av 28. februar 1997 nr 19, § 21-3, jf § 21-2.

uansett gjelder et prinsipp om forsvarlig saksbehandling; dvs. forvaltningsorganet må uansett, innenfor rammene av lovgivningen, sørge for at alle deler av saksbehandlingen blir fullt ut forsvarlig. Dette gjelder også for de deler av saksutredningsarbeidet som lovgiver kan ha lagt til parter og andre. En rutine som forutsetter at partene selv inngir hele beslutningsgrunnlaget, må derfor ha slike informasjons- og støttefunksjoner som sikrer at det ikke oppstår så mange feil at saksbehandlingen blir uforsvarlig. Hvor grensen for forsvarlighet går, avhenger selvsagt av en konkret vurdering, men det er neppe i samsvar med god forvaltningsskikk å balansere på grensen for hva som kan regnes som forsvarlig. Poenget er at kombinasjonen av utredningsprinsippet og prinsippet om forsvarlig saksbehandling, plasserer det grunnleggende ansvaret for saksutredning og øvrig saksbehandlingsoppgaver på forvaltningsorganet selv. Lovbestemmelser som plasserer oppgaver på andre enn forvaltningsorganet, fritar derfor ikke forvaltningsorganet fra dette ansvaret. I e-forvaltningen vil det ikke sjelden bli fastsatt en arbeidsdeling som innebærer at forvaltningsorganet, for å handle i samsvar med nevnte prinsipper, må sikre forsvarlig saksbehandling ved å tilby parter og andre informasjonssystemer som gjør dem i stand til å gjennomføre saksutredningsoppgavene uten fare for uakseptable feil. Utgangspunktet må være at desto mindre direkte befatning forvaltningsorganet har med å kontrollere opplysninger som parter inngir, desto bedre må støtten i form av informasjonssystemer mv være.

Når forvaltningens enkeltsaksbehandling og saksutredning gjelder fysiske personer, vil alle opplysninger i saken være knyttet til vedkommende person, og således være «personopplysninger» slik begrepet er definert i pol § 2 nr 1. I e-forvaltningen vil det dessuten skje «elektronisk behandling» av disse opplysningene, noe som innebærer at hele personopplysningsloven kommer til anvendelse.[14] Saksutredningsprosessen reguleres med andre ord av personopplysningsloven, og det er primært bestemmelsene i §§ 8 og 9 (rettslig grunnlag), §§ 11 (krav til formål og opplysningskvalitet mv), §12 (bruk av entydige identifikasjonsmidler), § 13 (informasjonssikkerhet), § 14 (internkontroll) og § 27 (sletting og retting av opplysninger mv) som regelmessig kommer til anvendelse.[15] I tillegg gjelder bestemmelsene i forvaltningsloven vedrørende saksutredning og foreleggelse av opplysninger for sakens parter, se fvl § 17.[16] Allerede

14 Se pol § 3 første ledd bokstav a, jf § 2 nr 2.

15 I tillegg gjelder selvsagt alltid de innledende bestemmelser med legaldefinisjoner mv, og bestemmelser vedrørende Datatilsynets og Personvernnemndas virksomhet mv.

16 Fvl § 16 om varsling av parter blir kortfattet trukket inn ved fremstillingen av § 17, og bestemmelsene i fvl § 15 om granskning, tas ikke med i denne diskusjonen fordi det representerer en problemstilling som ikke har generell relevans. Også granskning kan imidlertid lett inngå i e-forvaltningsløsninger.

av oversikten over aktuelle bestemmelser, kan leseren se at det er *personopplysningsloven og ikke forvaltningsloven* som inneholder den mest omfattende rettslige reguleringen av forvaltningens saksutredning når utredningen involverer personopplysninger. Nedenfor går jeg inn på de nevnte bestemmelsene for å formidle sammenhengen mellom bestemmelsene i de to lovene. Jeg går ikke inn på detaljspørsmål, men holder meg til hovedlinjene.

2.2 Hva skal ambisjonen for saksutredningsarbeidet være?

Fvl § 17 første ledd, første setning angir ambisjonsnivået for saksutredningen: «Forvaltningsorganet skal påse at saken er *så godt opplyst som mulig* før vedtak treffes.» (min kursiv). Bestemmelsen er vagt formulert, men angir noen helt sentrale rammer for saksutredningen og dermed for utforming av informasjonssystemer i den elektroniske forvaltningen. For det første gir bestemmelsen både uttrykk for utredningsprinsippet og forsvarlighetsprinsippet, ved at den fastsetter at det er forvaltningsorganet som skal opplyse saken, og at dette skal skje «så godt som mulig». Her skal jeg ikke gjenta innholdet av forvaltningsorganets ansvar, men jeg kommer tilbake til spørsmålet om kvalitetsstandarden «så godt som mulig».

Før jeg utdyper kvalitetsstandarden, vil jeg kort kommentere tidsangivelsen i bestemmelsen «før vedtak treffes». Formuleringen innebærer at saker skal opplyses slik at vedtaket blir korrekt uten at det skjer etterfølgende korreksjoner. Et forvaltningsorgan kan med andre ord ikke legge opp saksbehandlingen slik at den vet at behandlingsopplegget ikke gir tilstrekkelig resultat. Dette må forstås som et forbud mot å basere seg på at det vil skje feil som siden vil bli rettet opp etter klage fra parten eller ved omgjøring av vedtaket etter eget tiltak. Fvl § 17 innebærer derfor en ramme for utvikling og drift av IKT-baserte saksbehandlingsrutiner ved at bestemmelsen forbyr bruk av beslutningssystemer dersom disse inneholder kjente feil eller ufullstendigheter som ikke fanges opp av manuelle rutiner før formelt vedtak treffes. En kan for eksempel tenke seg at det er fristende å benytte en opplysning fra et annet forvaltningsorgan dersom definisjonen samsvarer 90 % med egen definisjon (for eksempel nesten likt inntektsbegrep). Dersom manuelle rutiner for å fange opp forskjellen er uforholdsmessig dyrt, kan det være fristende å basere saksbehandlingen på at endringer kan skje etter klage fra parten.[17] En slik rutine vil altså stride mot fvl § 17.

17 Forvaltningsorganet kan for eksempel tenkes å gi informasjon med oppfordring om å sjekke vedtaket på bestemte punkter.

Tidsangivelsen for kvalitetsstandarden bekreftes indirekte av personopplysningslovens krav til meldeplikt (§ 31) og konsesjonsplikt (§ 33),[18] sammenholdt med kvalitetskravene i § 11 første ledd bokstavene d og e. Melde- og konsesjonsplikten der kvalitetsvurderingen inngår skal iakttas *før* behandlingen av personopplysninger starter. Før personopplysninger benyttes for vedtaksformål må forvaltningsorganet med andre ord vurdere hvilke opplysningstyper som gir tilstrekkelig kvalitet for dette formålet.

Saker skal opplyses «så godt som mulig». Det er bred enighet om at dette må oppfattes som en retningslinje, snarere enn et definitivt krav. I forvaltningsrettslig litteratur er det primært situasjonsbestemte forhold som trekkes inn i diskusjonen om hvilke kvalitetskrav som gjelder. Således er det for eksempel lagt vekt på betydningen av saken for parten(e), viktigheten av en rask avgjørelse, forvaltningsorganets kompetanse, ressurssituasjon, restansemengde mv.[19] Slike ytre omstendigheter og rammebetingelser er særlig egnet for å angi hva som generelt må antas å være en rimelig ressursinnsats. Diskusjonen i forvaltningsrettslig litteratur sier imidlertid lite eller ingen ting om hvilke nærmere kvalitetskrav som kan stilles til *resultatet* av forvaltningens saksutredning. Når det gjelder den faktiske siden av beslutningsgrunnlaget, stiller imidlertid personopplysningsloven forholdsvis detaljerte krav til resultatet, dvs. til det materielle innholdet av vedtaket.

Pol § 11 første ledd bokstavene d og e, angir krav om at personopplysninger skal være tilstrekkelige, relevante, korrekte, oppdaterte og at de skal lagres i begrenset tid. Alle kravene skal vurderes ut i fra formålet med behandlingen av personopplysninger. For forvaltningen vil det innebære at det i kvalitetskravet i § 17 første ledd må innfortolkes et krav om at beslutningsgrunnlaget skal være så relevant, korrekt mv som formålet å treffe en konkret type enkeltvedtak krever. Dette innebærer at forvaltningsorganet ikke kan nøye seg med en overflatisk bedømmelse av hvor «godt» de opplyser sakene, men konkret må gå inn på en nærmere vurdering av de kvalitetsaspekter som er regnet opp i pol § 11 første ledd bokstavene d og e.[20]

I tillegg til § 11 kommer internkontrollbestemmelsen i pol § 14 inn og pålegger forvaltningsorganet å etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene til opplysningskvalitet. Bestemmelsen innebærer at vurderingen av opplysningskvalitet blir løftet opp

18 Meldeplikten vil i praksis spille størst rolle for forvaltningsorganer, fordi det er gjort unntak for konsesjonsplikten «for behandling av personopplysninger i organ for stat eller kommune når behandlingen har hjemmel i egen lov», se § 33 fjerde ledd.

19 Woxholth 1999, kommentarer til § 17 (4).

20 Dvs krav til personopplysninger som er tilstrekkelige, relevante, korrekte, oppdaterte, og lagret i avgrenset tid, alt i vurdert ut i fra formålet med behandlingen av opplysningene.

til systemnivået, slik at kvalitetssikringen ikke på lovlig måte kan begrenses til hver enkelt sak. Internkontrollprosessen skal ha som siktemål å avdekke behov for tiltak, og det grunnleggende er derfor selve kvalitetsanalysen. Konklusjonen kan derfor gjerne være at det ikke er behov for tiltak. Hvor dyptgripende kvalitetsvurderingene må være, kan til en viss grad avhenge av samme situasjonsbestemte forhold som er nevnt i forvaltningsrettslig litteratur knyttet til fvl § 17. Likevel kan ikke manglende kompetanse, ressurssituasjonen eller lignende frita forvaltningsorganet fra å gjennomføre systematisk gjennomgang av kvaliteten på de personopplysninger som legges til grunn for enkeltvedtak. Blant momenter som tilsier strenge krav til vurdering er betydningen for den enkelte av det vedtaket som skal treffes.

Med utgangspunkt i personopplysningsloven er det også grunn til å peke på andre konsekvenser av kvalitetskravene. Kravene i pol § 11 første ledd bokstavene d og e stilles ikke bare for å sikre riktige primærvedtak, men gjelder generelt og skal sikre at personopplysningene holder tilstrekkelig kvalitet også i forhold til enhver annen *sekundær* bruk, dvs for ethvert formål som opplysningene er innsamlet for. Forvaltningsorganet må derfor også vurdere kvaliteten i forhold til videre behandling av opplysninger, for eksempel i forhold til overføring av opplysningene til samarbeidende etat.

2.3 Rett til informasjon og kontradiksjon under saksforberedelsen

Både forvaltningsloven og personopplysningsloven bygger på en forutsetning om at den enkelte ønsker å beskytte sin rettsstilling, og gir derfor en rekke rettigheter til parter og registrerte personer. Personopplysningslovens formål er å ivareta personvernet, men lovens bestemmelser er godt egnet for også å ivareta andre rettslige interesser. Parter i forvaltningssaker vil alltid være «registrert» person, noe som i følge pol § 19 innebærer at parten skal gis informasjon når opplysninger om parten blir samlet inn direkte fra ham. Denne informasjonen skal typisk bli gitt i tilknytning til utfylling av søknadsskjema eller lignende, men kan også (delvis)[21] være aktuell å gi senere i saksbehandlingen dersom det blir hentet inn supplerende opplysninger. Bestemmelsen gjelder uavhengig av om personopplysninger gis etter pålegg eller skjer frivillig. Informasjonen etter pol § 19 skal omfatte:

21 Dersom informasjon allerede er gitt ved innledning av saksbehandlingen, kan senere informasjon ofte begrenses til å gjelde spørsmålet om frivillighet og utlevering. Forutsetningen er selvsagt at det ikke foreligger endringer i andre opplysninger.

- hvem som er behandlingsansvarlig og hvem som har daglig ansvar for behandling av opplysningene,
- om avgivelsen av opplysningene er frivillig,
- formålet med behandlingen,
- om opplysningene blir utlevert og eventuelt til hvem, og
- annet som gjør den registrerte istand til å benytte rettighetene etter personopplysningsloven.

Fvl § 14 regulerer tilfelle der et forvaltningsorgan *pålegger* en person å gi opplysninger, dvs når innsamlingen av personopplysninger mv ikke er frivillig. Personen kan være part eller en annen som har opplysninger som forvaltningsorganet ønsker. I slike tilfelle fastsetter bestemmelsen at forvaltningsorganet uoppfordret skal oppgi hjemmelen for pålegget. Bestemmelsen gir i slike situasjoner en rettssikkerhetsgaranti ved at det gis en rett til å påklage kravet om å gi opplysninger. En slik klage har normalt oppsettende virkning. Ved innsamling av personopplysninger etter pol § 19 stilles det ikke direkte krav om angivelse av rettslig grunnlag (jf pol §§ 8 og 9), dvs. av om behandling av personopplysninger er basert på lovhjemmel, samtykke eller «nødvendig grunn».[22] Imidlertid kan slik informasjon ofte være påkrevet for å sette «den registrerte i stand til å benytte rettighetene etter personopplysningsloven», jf § 19 første ledd bokstav e.

Samlet sett innebærer fvl § 14 sammenholdt med pol § 19 at forvaltningsorganet har en langt videre informasjonsplikt enn det som fremgår av fvl § 14. Det kan dessuten være behov for mer utfyllende informasjon om rettslig grunnlag enn informasjon om lovhjemmel når noen pålegges å gi personopplysninger.

Forvaltningsloven har for øvrig ingen særlig bestemmelse om innhenting av opplysninger fra partene, så på dette punktet er pol § 19 supplerende og skaper ingen problemer i forhold til forvaltningslovens bestemmelser. Derimot regulerer både fvl § 17 annet og tredje ledd og pol § 20 situasjoner der forvaltningen mottar saksopplysninger fra *andre* enn parten.[23] Etter fvl § 17 er det to situasjoner som er aktuelle. For det første regulerer § 17 annet ledd tilfelle der forvaltningsorganet mottar opplysninger om *partens person eller virksomhet*, dvs opplysninger som stort sett må regnes som personopplysninger om parten. jf pol § 2 nr 1. I tillegg fastsetter tredje ledd at forvaltningsorganet *bør* gjøre partene kjent med andre opplysninger som er av vesentlig betydning for saken

22 Indirekte vil det rettslige grunnlaget fremgå fordi det skal opplyses om det er frivillig eller ikke å gi fra seg personopplysninger, se § 19 første ledd bokstav d. Er det frivillig vil grunnlaget som oftest være samtykke, jf § 2 nr 7.

23 Det forutsettes det at parten har innsynsrett i opplysningene, jf fvl §§ 18 og 19.

og som parten antas å ha grunnlag og interesse for å uttale seg om. Denne siste bestemmelsen vil imidlertid ikke bli nærmere drøftet her.

Plikten etter fvl § 17 annet ledd til å forelegge personopplysninger i saken gjelder ikke dersom:

- opplysningen tilsvarer slike opplysninger som parten tidligere har gitt eller kontrollert, eller
- det ikke har avgjørende betydning for vedtaket at opplysningene blir forelagt parten under saksforberedelsen, eller
- parten oppholder seg på ukjent sted, eller
- det er påkrevet med en rask avgjørelse i saken.

Oppregningen i kulepunktene ovenfor tilsvarer ikke rekkefølgen i § 17, men er gruppert etter type unntak. I de to første punktene kan unntak gjøres etter en vurdering av opplysningenes innhold, mens de to siste punktene gjelder den ytre situasjonen.

Foreleggelsesplikten etter fvl § 17 annet ledd inneholder implisitt en plikt for forvaltningsorganet til også å informere parten om eksistensen av opplysningene. Forvaltningsorganets plikt omfatter med andre ord både å gi informasjon om eksistensen av opplysningene, og å gjøre disse opplysningene tilgjengelig for parten. Etter pol § 20 har forvaltningsorganet kun en plikt til å informere parten. Denne informasjonen skal omfatte i) hvilke opplysninger som samles inn og ii) opplysninger om denne informasjonsinnsamlingen, tilsvarende slike opplysninger som skal gis etter pol § 19 (jf ovenfor). Det fremgår ikke direkte av lovteksten eller forarbeider om informasjonen kun skal gjelde opplysningstypen eller om det skal informeres om de konkrete opplysningene. Spørsmålet er for eksempel om varselet skal være "Vi har mottatt opplysninger om din inntekt", eller om den skal være "Vi har mottatt opplysninger om at din inntekt er kr 300.000,- per år". Fordi forarbeidene forutsetter at informasjonen i enkelte tilfelle kan gis kollektivt, er det imidlertid grunn til å anta at det kun er opplysnings*typen* som omfattes av plikten til å gi informasjon. Ut i fra offentlighetsprinsippet og en retningslinje om meroffentlighet, har forvaltningsorganet imidlertid ofte anledning til å gi parten informasjon om de konkrete opplysningene som er mottatt. I så fall blir informasjonsplikten etter pol § 20 langt på vei sammenfallende med foreleggelsesplikten etter fvl § 17 annet ledd. Uansett vil situasjonen normalt være at den registrerte har innsynsrett i opplysningene, jf pol § 18 og fvl § 18. Dersom det kun gis informasjon om opplysningstyper, kan parten derfor skaffe seg kunnskap om de konkrete opplysningene ved å begjære innsyn.

Også pol § 20 stiller opp unntaksalternativer som beskriver når det ikke eksisterer en plikt til å gi informasjon til den registrerte personen (parten). Unntak gjelder dersom:

- Innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov, eller
- det er på det rene at den registrerte allerede kjenner til informasjonen varslet skal inneholde, eller
- varsling er umulig eller uforholdsmessig vanskelig.

Også her har jeg valgt en rekkefølge på punktene som avviker noe fra lovens. Poenget er å gruppere for å få frem at de to første punktene gjelder innholdsmessige kriterier, mens det siste punktet refererer til situasjonsbestemte vilkår. Samlet sett gir fvl § 17 annet ledd og pol § 20 denne unntaksstrukturen:

	Fvl § 17, 2. ledd	**Pol § 20**
Unntak i henhold til innhold:		
	Opplysningen er slike som parten tidligere har gitt eller kontrollert	Den registrerte er allerede kjenner til informasjonen
		Innsamlingen av opplysningene er uttrykkelig fastsatt i lov
	Forleggelse av opplysningene er ikke avgjørende betydning for vedtaket	
Unntak i henhold til situasjon:		
	Parten oppholder seg på ukjent sted	Varsling er umulig eller uforholds-messig vanskelig
	Det er påkrevet med en rask avgjørelse i saken	

Tabellen illustrerer at to sett av unntaksvilkårene etter de to lovene har et innhold som i meget stor grad harmonerer med hverandre. Dette gjelder for det første tilfelle der parten allerede kjenner opplysningene. Pol § 20 angir et resultat (kjennskap), mens § 17 annet ledd angir to hendelser som impliserer et slikt kjennskap. I dette ligger det muligheter for forskjellige resultater; for eksempel gjelder det i utgangspunktet ikke unntak etter fvl § 17 annet ledd dersom forvaltningsorganet er kjent med at parten faktisk har fått tilgang til opplysnin-

gene av andre, men uten at kunnskap om at opplysningene er kontrollert av parten. Intensjonen bak unntaksbestemmelsene i forvaltningsloven er trolig å angi en kvalifisert form for kjennskap, mens det etter pol § 20 ikke forutsettes noe om at opplysningene faktisk er vurdert av den registrerte (parten). Hadde lovgiver sett de to vilkårene i sammenheng, er det imidlertid tvilsomt om slike forskjeller hadde vært opprettholdt.

Det andre paret unntaksvilkår som tilsvarer hverandre, gjelder praktiske, situasjonsbestemte vanskeligheter med å gi informasjon til parten. Igjen er forvaltningsloven konkret ved at den angir en situasjon da den praktiske vanskeligheten oppstår, mens personopplysningsloven i stedet angir et resultat (umulighet eller uforholdsmessig vanskelig). Jeg vil ikke her foreta en full gjennomgang av hvorledes de to bestemmelsene bør fortolkes, men nøyer meg med å peke på at ordlydene gir noen viktige forskjeller. Særlig gjelder dette spørsmålet om arbeidsinnsats i tilfelle informasjonen må gis til et stort antall personer. Slike situasjoner er omfattet av pol § 20 «uforholdsmessig vanskelig», men er ikke direkte omfattet av unntakene i § 17 annet ledd. I slike tilfelle er det imidlertid grunn til å anta at alternativet som knytter seg til behovet for rask avgjørelse vil bli vurdert i lys av den arbeidsinnsatsen som kreves. Resultatet kan derfor lett bli det samme etter de to unntaksbestemmelsene.

3. Taushetsplikt og informasjonssikkerhet

3.1 Innledning

Forvaltningsloven inneholder detaljerte bestemmelser om taushetsplikt for den som utfører tjeneste eller arbeid for et forvaltningsorgan, se fvl §§ 13 – 13f. Taushetsplikten gjelder både «noens personlige forhold» og tekniske innretninger, fremgangsmåter mv. Her skal jeg avgrense meg til å drøfte spørsmål knyttet til taushetsplikt vedrørende «noens personlige forhold».

Personopplysningsloven inneholder ikke andre taushetspliktregler enn en særbestemmelse i § 45 om tilsynsmyndighetenes taushetsplikt. Selv om ivaretakelse av konfidensialitet er et sentralt hensyn i personopplysningsretten, er dette hensynet primært ivaretatt *utenfor* personopplysningsloven ved hjelp av regler om taushetsplikt. Personopplysningsloven med tilhørende forskrift inneholder imidlertid andre typer konfidensialitetsvern som må ses i sammenheng med taushetsplikter, jf særlig fvl § 13 flg. For å ivareta krav til konfidensialitet, må forvaltningsorganer som behandler personopplysninger både forholde seg til taushetspliktbestemmelser i forvaltningslovgivningen *og* bestemmelser i personopplysningsloven.

Bestemmelsene i personopplysningsloven som kan sies å understøtte konfidensialitet, er hovedsakelig av to slag: Dels gjelder det bestemmelser som legger begrensninger på retten til å aksessere personopplysninger, og dels bestemmelser som er satt for å sikre at bestemmelser vedrørende begrensninger i tilgang på personopplysninger (taushetsplikt mv) faktisk blir etterlevet. Denne siste kategorien bestemmelser benevner jeg «informasjonssikkerhetsbestemmelser». Før jeg kommer nærmere inn på de to nevnte regelkategoriene, er det imidlertid nødvendig å gi en nærmere analyse av det som skal beskyttes; nemlig «noens personlige forhold» og «personopplysninger».

3.2 «Noens personlige forhold» som «personopplysning»

«Noens personlige forhold» er en egen kategori opplysninger som ikke uten videre passer inn i, eller har et avklaret forhold til, den nært beslektete terminologien i personopplysningsloven. Begrepet ligger antagelig innenfor begrepet «personopplysning» i den forstand at det kun er tale om opplysninger om fysiske personer. Ved avgrensingen av «noens personlige forhold» er det vanlig å gå kasuistisk til verks for å undersøke hvor grensen går i forhold til opplysninger om personer som ikke er underlagt taushetsplikt.[24] En generell retningslinje er at opplysninger som det er vanlig å ønske å holde for seg selv er underlagt taushetsplikt.[25] Dette gir en situasjon der spørsmålet om taushetsplikt må avgjøres konkret for hver opplysningstype i konkrete kontekster, og det gir en betydelig gråsone der det kan være berettiget usikkerhet mht om det foreligger taushetspliktige personopplysninger eller ikke. Definisjonen av «personopplysning» er ikke på samme måte avhengig av situasjonsbestemte vurderinger. Dette begrepet må primært avgrenses i forhold til hvor direkte en opplysning er knyttet til en fysisk person, og hvor sikkert og entydig den aktuelle personen kan identifiseres.[26]

Dersom vi ser «noen personlige forhold» som en underkategori av «personopplysning», genererer dette en rekke spørsmål som det ikke uten videre er lett å ta stilling til på grunnlag av forvaltningsloven:

- Gjelder taushetsplikten bare for levende personer?
- Må de personlige forholdene faktisk være koplet til en person, eller er det nok at opplysningene er potensielle?

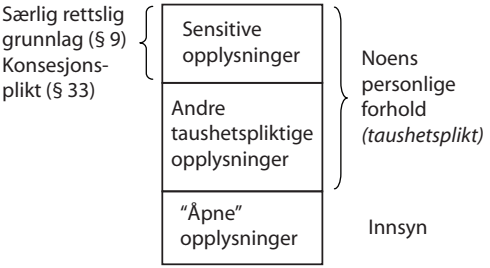
24 Se f.eks. Lovavdelingens uttalelse vedrørende forståelsen av fvl § 13 og § 13a, Saksnummer: 1998/10047 E AS/ØØ, datert 19.11.1998.

25 Se Woxholth 1999 s 204 flg.

26 Avgrensingen av begrepet personopplysning er for eksempel diskutert i Schartum og Bygrave 2004, s 106 – 122.

- Hvor indirekte og sammensatt kan koplingen mellom personlige forhold og personen være?[27]
- Hvor sikker må tilknytningen mellom opplysningen om personlige forhold og personen være?
- Hvor sikker/klar må den aktuelle personens identitet være?

Her vil jeg ikke drøfte spørsmålene nærmere, men nøyer meg med å peke på at dette uansett er generelt relevante spørsmål å stille ved etterlevelse av taushetsplikt iflg. fvl § 13.[28] Spørsmål knyttet til avgrensingen av «personopplysning» etter pol § 2 nr 1 har et informasjonsvitenskapelig preg; svarene er i stor grad avhengig av det generelle opplegget for informasjonsbehandlingen, og i mindre grad knyttet til konkrete, materielle vurderinger av opplysningenes innhold. Mens forvaltningsloven legger til rette for konkrete, individuelle vurderinger, legger personopplysningsloven primært til rette for vurderinger av generelle opplegg for behandling av personopplysninger, dvs. på systemnivå.



Det er ingen formell forbindelse mellom «noens personlige forhold» og «personopplysning», dvs. lovgiver har ikke i lov eller forarbeider forholdt de to begrepene til hverandre. Imidlertid skaper det faktum at begge lover gjelder for forvaltningens saksbehandling mv et praktisk behov for å se de to begrepene i sammenheng. Forvaltningsorganer må med andre ord vite hvilke personopplysninger de har, og hvilke nærmere regler som gjelder for opplysningene. Med en slik generell tilnærming blir spørsmålet om taushetsplikt vedrørende personlige

27 Jf uttalelse fra Justisdepartementets lovavdeling (jnr 3098/82) der det ble uttalt at «… opplysninger som knytter seg direkte til en person, omfattes av taushetsplikten. Men også enkelte andre opplysninger om forhold som er egnet til å karakterisere vedkommende, må anses for å gjelde vedkommendes personlige forhold.» Mens personopplysninger utvilsomt også omfatter opplysninger som indirekte er knyttet til person, kreves det med andre ord primært direkte tilknytning etter forvaltningsloven.

28 Likevel har slike tolkningsspørsmål neppe vært særlig betydningsfulle i forvaltningsrettslig teori.

forhold en åpenbar del av personopplysningsvernet, dvs. det blir nødvendig å forstå taushetsplikten innenfor en personopplysningsrettslig ramme.

Som nevnt er det nærliggende å forstå «noens personlige forhold» som en underkategori av «personopplysning». Personopplysningsloven inneholder imidlertid også angivelse av en annen delmengde; «sensitive personopplysninger». I motsetning til forvaltningslovens generelle og vage angivelser, er denne angivelsen temmelig spesifikk. Således definerer pol § 2 nr 7 i alt fem opplysningstyper som «sensitive»; for eksempel opplysninger vedrørende helse, seksuelle forhold, opplysninger om politiske/filosofiske/religiøse oppfatninger mv.

Igjen oppstår spørsmålet om forholdet mellom slike sensitive personopplysninger og «noens personlige forhold» etter forvaltningsloven. Er sensitive personopplysninger en delmengde av de opplysninger som gjelder personlige forhold og som derfor er underlagt taushetsplikt? I hovedsak er svaret trolig ja på dette spørsmålet, men bildet er ikke entydig. For eksempel er det tvilsomt om den sensitive personopplysningen om fagforeningsmedlemsskap (jf pol § 2 nr 8 bokstav e) gjelder noens personlige forhold og underlagt taushetsplikt â i hvert fall ikke dersom det har vært åpenhet om medlemsskapet. Heller ikke opplysninger om straffbare forhold vil alltid være underlagt taushetsplikt etter fvl § 13.[29] Selv om det lagt på vei er slik at «sensitive personopplysninger» kan ses som en delmengde av «noens personlige forhold», er dette derfor neppe en unntaksfri regel. Årsaken er formodentlig primært at vurderingen etter § 13 er langt mer konkret enn etter pol § 2 nr 8, og at det etter forvaltningsloven stilles strengere krav til direkte og klarere tilknytning mellom opplysningen og en fysisk person enn etter personopplysningsloven.

Mitt poeng er at fvl § 13 bygger på en begrepsbruk som passer dårlig inn i forhold til definisjonen av «personopplysning» i pol § 2 nr. 1 og nr. 8 – og omvendt. I hvilken grad og på hvilken måte det er mulig å etablere en rimelig grad av sammenheng mellom de to tilnærmingene, tar jeg ikke stilling til her. Der er imidlertid nærliggende å tro at det primært er forvaltningslovens bestemmelser som må tilpasses definisjonene i personopplysningsloven. Årsaken er at pol § 2 nr. 1 og nr. 8 er knyttet til personverndirektivet,[30] og dermed til Norges forpliktelser innen EØS-avtalen.

29 Se Lovavdelingens uttalelse, saksnummer: 1998/10047, med videre referanser.
30 Direktiv 46/95/EU.

3.3 Bestemmelser i personopplysningsloven med betydning for forvaltningens tilgang til personopplysninger

Taushetspliktreglene i forvaltningsloven tar utgangspunkt i at personer i forvaltningen har fått kunnskap om personopplysninger om personlige forhold. Situasjonen som forutsettes er med andre ord at personer i forvaltningsorganet kognitivt har tilegnet seg opplysningene, og forutsetter ikke at opplysningene er registrert hos forvaltningsorganet eller lignende. Forvaltningsloven regulerer i liten grad spørsmål vedrørende den primære innsamlingen/registreringen av opplysninger og vilkår for videre bruk innenfor rammene av taushetsplikt. På disse punktene supplerer personopplysningsloven på måter som innebærer et videre konfidensialitetsvern enn det regler om taushetsplikt gir.

For at forvaltningsorganet over hode skal komme i besittelse av personopplysninger som det kan gjelde taushetsplikt for, må de i følge pol § 8 ha rettslig grunnlag for dette.[31] Uten rettslig grunnlag vil det i utgangspunktet være forbudt for forvaltningsorganet å behandle personopplysninger elektronisk eller i et personregister. Mulige grunnlag er at:

- det er hjemmel for behandlingen i eller i medhold av lov,
- det foreligger samtykke fra den registrerte personen,
- det foreligger en slik nødvendig grunn som personopplysningsloven angir,
- opplysningene er slike som den registrerte selv frivillig har gjort alminnelig kjent.[32]

Her vil jeg ikke gjennomgå de krav som må stilles for at hvert av de mulige grunnlagene kan sies å foreligge.[33] Poenget her er at disse kravene kan gjøre at det ikke bare er ulovlig å viderebringe personopplysninger, men at det i utgangspunktet kan være ulovlig for forvaltningsorganet å innhente og besitte opplysningene. Ulovlig besittelse av personopplysninger kan særlig tenkes å skje på to måter: i) Forvaltningens innsamling av opplysninger tilfredsstiller ikke vilkårene i § 8 (det er for eksempel innhentet samtykke, men kravene til gyldig samtykkeerklæring i § 2 nr 7 er ikke tilfredsstilt), og ii) det eksisterer intet mulig rettslig grunnlag for innhenting og videre behandling av opplysningene. Under

31 Det gjelder egne krav til rettslig grunnlag etter pol § 9 for behandling av slike opplysninger som i pol § 2 nr 7 er definert som sensitive, men dette kommer jeg ikke nærmere inn på her.

32 Dette alternativet er ikke tatt inn i pol § 8, og er kun gjort eksplisitt for sensitive personopplysninger i § 9 første ledd bokstav d. Når loven aksepterer dette som grunnlag for behandling av sensitive opplysninger, antar jeg det samme må gjelde for ikke sensitive opplysninger som generelt antas å innebære mindre risiko for krenkelser av personvern.

33 Se om dette i Schartum og Bygrave 2004, s 130 – 137.

det siste tilfellet hører også situasjoner der det rettslige grunnlaget har falt bort (en lovhjemmel er opphevet, samtykke er trukket tilbake eller nødvendighetsgrunn har opphørt og eksistere).

Krav til rettslig grunnlag for å behandle personopplysninger er særlig viktig i tilknytning til forvaltningens tjenester på Internett. Fordi rutinene for informasjonsinnsamling delvis kan automatiseres og manuelt arbeid i stor grad kan utføres av de registrerte selv, kan forvaltningens apetitt på personopplysninger bli større enn det enkeltsaksbehandlingen krever. For forvaltningsorganer får pol § 8 særlig betydning for opplysninger som innhentes i tillegg til det enkeltsaksbehandlingen krever. Registrering av CV på Arbeidsmarkedsetatens hjemmeside,[34] er et eksempel på en tjeneste der samtykke skulle ha vært innhentet og der det ikke foreligger noe annet rettslig grunnlag.[35] Selv om etaten overholder sin taushetsplikt, overtrer de uansett loven fordi opplysningene ikke er innhentet på lovlig måte.

Det andre elementet i personopplysningsloven som kan ses som et konfidensialitetsvern som supplerer taushetsplikten i forvaltningsloven, er kravet om at enhver personopplysning kun skal behandles for bestemte, på forhånd angitte *formål*, se pol § 11 første ledd bokstav b, jf bokstav c.[36] Selv om opplysningen er lovlig innhentet, og personene i forvaltningsorganet overholder sin taushetsplikt, innebærer bestemmelsen at det er begrensninger med hensyn til hva opplysningene kan brukes til.[37] Formålet for behandlingen av personopplysninger skal angis før behandlingen begynner, dvs før innhenting av opplysninger skjer.[38] Dersom det rettslige grunnlaget er lov eller samtykke, vil formålet fremgå av henholdsvis lovteksten mv og/eller samtykkeerklæringen med tilhørende informasjon. Er det en «nødvendig grunn» som utgjør den rettslige basisen (jf § 8 første ledd bokstavene a – f), må forvaltningsorganet selv fastsette hva formålet er, i samsvar med den grunnen som er påberopt.[39]

---

34 Se https://www.aetat.no/sbl/as/velgRegistrering.do.

35 Arbeidsmarkedslovens (lov av 10. desember 2004 nr. 76) § 10 gir rett til å registrere seg som arbeidssøker. Registrering av CV er imidlertid en tilleggstjeneste for den som ikke ønsker registrering etter § 10. Uansett angir ikke loven noe om hvilke opplysninger som registrering av arbeidssøker eller CV kan omfatte.

36 Se om formålsbestemthetsprinsippet i Bygrave 2002 s 61.

37 Formålsbegrensning kan også ses som en mulig begrunnelse for taushetsplikt, fordi utlevering til uvedkommende meget ofte vil innebære at opplysningene vil kunne bli brukt til andre og ukontrollerbare formål.

38 Dersom det foreligger meldeplikt for vedkommende behandling av personopplysninger innebærer dette at formålet senest må fastsettes 30 dager før behandlingen starter, se pol § 31 annet ledd, jf. § 32 første ledd bokstav d.

39 Pol § 11 første ledd bokstav c åpner for at formålet kan endres, men denne muligheten kommer jeg ikke nærmere inn på her.

Krav til formålsangivelse etter personopplysningsloven innebærer en dobbelt begrensning på bruken av personopplysningene. For det første begrenser det bruken for den som lovlig har samlet inn opplysningene. For det andre kan formålsangivelsen trolig få konsekvenser for anvendelsen av unntaksbestemmelsene fra taushetsplikt i forvaltningsloven:[40] Når grensene for taushetsplikt angis i forvaltningsloven, gjøres det på samme måte som i personopplysningsloven, ved at det i stor grad anvendes formålskriterier. Således heter det i § 13b første ledd nr 2 at taushetsplikten ikke er til hinder «for å oppnå det *formål* de er gitt eller innhentet for» (min kursiv). I tillegg opererer forvaltningsloven med en rekke sekundære formål som opplysninger kan benyttes til uten hinder av taushetsplikt, for eksempel til veiledning i andre forvaltningssaker, statistikk og forskning. Selv om formuleringene ikke benytter ordet «formål», er det gjennomgående en formålstenkning som preger denne grenseoppgaven for betydningen av taushetsplikt.

Forvaltningslovens bestemmelser om taushetsplikt kan med andre ord sies å være knyttet til visse primære og sekundære formål for bruken av den kunnskap/de opplysninger som forvaltningen besitter. På den måten er det stor grad av samsvar mellom tenkningen bak fvl §§ 13 ā13f og pol § 11 bokstav b, jf c. Også på dette punktet er det imidlertid en viktig forskjell ved at forvaltningsloven primært forutsetter konkrete vurderinger av formål mens personopplysningsloven forutsetter vurderinger på systemnivå: Mens personopplysningsloven krever at formålet må angis på forhånd, er det intet tilsvarende krav etter forvaltningsloven. Skal en følge personopplysningsloven må for eksempel forskning være angitt som formål for behandling av personopplysninger for at dette skal være lovlig bruk. Etter fvl § 13d kan forvaltningsorganet ta stilling til spørsmålet om bruk til forskning på et hvilket som helst tidspunkt («Når det finnes rimelig og ikke medfører uforholdsmessig ulempe for andre interesser, kan departementet bestemme …»). Avgjørelsen er med andre ord konkret og situasjonsbestemt. Tilsvarende situasjon oppstår i forhold til flere andre sekundærformål.

Det foreligger ikke nødvendigvis noen motstrid mellom bestemmelsene i pol § 11 første ledd bokstav b, jf c og fvl § 13d (og tilsvarende bestemmelser). Sammenholdt kan de to bestemmelsene forstås slik at det først kan fastsettes at personopplysninger (f.eks.) kan behandles for forskningsformål (systemnivå), og at forvaltningsorganet innenfor denne rammen deretter konkret kan ta stilling til om det skal gjøres unntak fra taushetsplikten for det enkelte forskningsprosjektet. I rettspolitisk perspektiv kan imidlertid også andre løsninger være

40 Det kan for eksempel på bestemte vilkår gjøres unntak for taushetsplikt når formålet er forskning, se forvaltningsloven § 13d.

ønskelige. Uansett er forholdet mellom generelle formålsbegrensninger i personopplysningsloven og angivelse av formål i forvaltningsloven vedrørende grensene for taushetsplikt, eksempel på uavklarte tolkningsspørsmål i møte mellom de to lovene.

3.4 Bestemmelser om informasjonssikkerhet

Taushetsplikt gjelder den enkelte person som får kunnskap om taushetsbelagte forhold. Forvaltningsorganet har plikt til å gjøre personene kjent med taushetsplikten, og til å oppbevare taushetsbelagte opplysninger på en betryggende måte, se fvl § 13c første og annet ledd.[41] Loven legger med andre ord også noen forsiktige plikter på forvaltningsorganet (og ikke bare på enkeltpersoner). I kontrast til dette legger personopplysningsloven bare plikter på forvaltningsorganet (den «behandlingsansvarlige»).[42] Pol § 13 pålegger således forvaltningsorganet å sørge for tilfredsstillende konfidensialitet ved behandling av personopplysninger, og bestemmer at tiltakene skal være planlagte, systematiske og dokumenterte. Heller ikke på dette punktet vil jeg gå nærmere inn i de detaljerte kravene. Jeg vil nøye meg med å peke på at det i forskrift er satt krav til nærmere fremgangsmåter for dette arbeidet, og at det herunder er stilt krav til gjennomføring av risikovurdering.[43] De forpliktelser for forvaltningsorganet som følger av fvl § 13c om sikring av taushetsplikt, suppleres med andre ord på vesentlige måter av pol § 13 med forskrifter.

Mens forvaltningsloven kun representerer en enkel og ufullstendig tilnærming til informasjonssikkerhet (se fvl § 13c), stiller pol § 13 opp langt mer vidtfavnende krav. Etter sist nevnte bestemmelse skal således også opplysningers integritet og tilgjengelighet sikres. Personopplysninger som et forvaltningsorgan behandler skal med andre ord sikres mot uautorisert endring og opplysningene skal være tilgjengelige for de formål de er innsamlet for. De samme kravene til planlagte, systematiske og dokumenterte tiltak gjelder her som ved sikring av konfidensialitet. I tillegg finnes detaljerte krav i forskrift.

41 Departementer kan også gi pålegg om bruk av taushetsplikterklæringer, se fvl § 13c første ledd.

42 En behandlingsansvarlig kan generelt sett være en enkeltperson, men innenfor offentlig forvaltning er dette upraktisk. Tilsvarende plikter som for den behandlingsansvarlige gjelder for den som behandler personopplysninger på den behandlingsansvarliges vegne («databehandler»), dvs i tilfelle behandling av opplysningene er satt bort (outsourcet) til andre, se pol § 13 første ledd.

43 Se personopplysningsforskriften (forskrift av 15. desember 2000 nr 1265), kapittel 2, særlig § 2-4 om risikovurdering.

Spesifikke krav til sikring av *elektronisk kommunikasjon* mellom forvaltningsorganer og mellom forvaltningsorganer og den enkelte, er gitt i forskrift med hjemmel i fvl § 15a.[44] Her er det delvis gitt regler for å beskytte taushetspliktbelagte opplysninger (§§ 5 og 24), og forskriftens § 13 angir enkelte generelle krav til forvaltningsorganers informasjonssikkerhetsarbeid: «Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten.» I denne bestemmelsen er det dessuten gitt en henvisning til sikkerhetskravene etter pol § 13 med forskrifter, dvs til bestemmelser som gjelder mer enn ivaretakelse av taushetsplikt.[45] eForvaltningsforskriften er med andre ord et eksempel på at departementet har fastsatt regler om informasjonssikkerhet der koplingen til personopplysningsregelverket er gjort tydelig. Dette er imidlertid bare gjort for elektronisk kommunikasjon og ikke for all den behandling av opplysninger som skjer innenfor rammene av forvaltningsorganet. Reguleringen blir derfor fragmentarisk og høyst ufullstendig.

4. Innsyn og åpenhet

Forvaltningsloven §§ 18 og 19 inneholder bestemmelser om rett for parter til å kreve innsyn i sakens dokumenter. Innsynsretten omfatter i utgangspunktet enhver opplysning i saken, herunder personopplysninger om andre og opplysninger om egen person. Opplysninger om egen person som forvaltningsorganet mottar fra andre, skal som hovedregel forelegges parten (jf § 17 annet ledd). Når det imidlertid gjelder opplysninger som er omfattet av unntak fra denne plikten, og opplysninger som parten selv har inngitt, er parten henvist til å kreve innsyn for å få tilgang til det samlede beslutningsgrunnlaget. I utgangspunktet vil det i slike tilfelle normalt være reglene om partsinnsyn som er mest hensiktsmessig for parten å gjøre bruk av fordi opplysningene her inngår i en sakspesifikk kontekst. I den elektroniske forvaltningen er det imidlertid ofte en ambisjon om å benytte opplysninger til flere formål. Opplysning om en persons inntekter, forsørgelsesbyrde mv vil med andre ord kunne inngå i flere avgjorte, aktuelle og/eller fremtidige enkeltvedtak hos forskjellige forvaltningsorganer. En slik utvikling kan begrunne at det er viktigere enn tidligere å få tilgang til opplysningene uavhengig av kontekst, eller samtidig i forhold til flere saksforhold.

Når det gjelder enkeltsaksbehandling vil særlig tilgang til egne personopplysninger være verdifullt for den som vil orientere seg om tidligere, aktuelt og

44 Se eForvaltningsforskriften (forskrift av 25. juni 2004 nr. 988).
45 Se eForvaltningsforskriften § 13 tredje ledd bokstav g.

potensielt beslutningsgrunnlag hos forvaltningsorganer. I så fall vil innsynsrettighetene etter pol § 18 jf § 23 være av stor betydning som et supplement til partsinnsyn etter fvl § 18. For det første vil den individuelle innsynsretten i henhold til pol § 18 annet ledd gi tilgang til alle opplysninger om vedkommende person, uavhengig av mer spesifikke saklige sammenhenger. På den måten kan det bli mulig å skaffe oversikt over eventuelle feil, inkonsistenser og ufullstendigheter i de foreliggende personopplysningene, og parten kan kontrollere om forvaltningsorganet har opplysninger om personen som det vil være usaklig å vektlegge. Ved å benytte partsinnsyn og innsyn for registrerte personer i kombinasjon, kan det med andre ord bli lettere for parter å skaffe informasjon for å ivareta egne rettslige interesser.

I tillegg til partsinnsyn etter fvl § 18 og innsyn i egne opplysninger etter pol § 18 annet ledd, har enhver rett til å få innsyn i bestemte opplysninger som beskriver behandlingen av personopplysninger, se § 18 første ledd. I samsvar med personverndirektivet omfatter dette:[46]

- hvem som er behandlingsansvarlig og hvem som har daglig ansvar for behandling av opplysningene,
- formålet med behandlingen,
- beskrivelser av hvilke typer personopplysninger som behandles,
- hvor opplysningene er hentet fra,
- om opplysningene blir utlevert og eventuelt til hvem,

Denne delen av innsynsretten gjelder for hver «bestemt[e] type behandling». Beskrivelse av en bestemt type behandling som leder frem til enkeltvedtak, vil derfor innebære en nærmere beskrivelse av vedkommende beslutningssystem/-rutine som følges i saker innen vedkommende forvaltningsmyndighet. Dersom noen søker arbeidsledighetstrygd, har vedkommende med andre ord rett til å få en beskrivelse som viser om arbeidskontoret innhenter opplysninger fra andre (og fra hvem), om opplysningene blir anvendt for flere formål (vedtak om sosialhjelp, iligning av skatt mv.), og om opplysningene (selve vedtakene og det faktiske grunnlaget for vedtak) oversendes andre (i offentlig eller privat sektor). Tilsvarende informasjon kan enhver kreve innsyn i med hjemmel i offentleglova[47] § 3. Forutsetningen er imidlertid at det faktisk foreligger et saksdokument som inneholder slike beskrivelser. Pol § 18 første ledd gjelder derimot uavhengig av om opplysningene foreligger som dokument eller ikke,

46 Opplysningene tilsvarer langt på vei den informasjon som skal gis etter pol §§ 19 og 20, jf avsnitt 2.3 (ovenfor).

47 Lov om rett til innsyn i dokument i offentleg verksemd av 19. mai 2006 nr 16.

og er derfor en sikker vei til kunnskap om vesentlige deler av beslutningsprosesser som for eksempel leder frem til enkeltvedtak.

Med den nære forbindelsen det er mellom partsinnsyn ifølge bestemmelser i forvaltningsloven og individuelt innsyn med hjemmel i personopplysningsloven, er det etter min mening uheldig at de to bestemmelsene ikke er mer direkte relatert til hverandre i selve lovteksten. Jeg mener særlig det kan være ønskelig dersom forvaltningsloven fikk en henvisning til pol § 18. Det kan på tilsvarende måte i og for seg reises kritikk mot at det ikke er henvisninger fra innsynsbestemmelsen i fvl § 18 til hovedregelen i offentleglova § 3. Også allmennhetens innsyn etter offl § 3 kan sies å supplere fvl § 18 på en slik måte at parter i forvaltningssaker også bør gjøres kjent med disse innsynsrettighetene. Likevel må det sies at innsynsrettigheter etter personopplysningsloven normalt vil ha et langt større potensiale i forhold til enkeltvedtak. Årsaken er at det individuelle innsynet gjelder opplysninger om parten selv samt opplysninger som beskriver hvorledes opplysninger om parten vil bli behandlet i tilknytning til og frem mot et enkeltvedtak.

Personvern er ofte assosiert med konfidensialitet og skjerming mot innsyn, og dette er selvfølgelig viktig i forhold til innsyn i personopplysninger fra andre enn vedkommende person selv. Da personopplysningsloven ble vedtatt, tok lovgiver derfor inn en bestemmelse som skulle garantere at loven ikke «begrenser […] innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger.» Samtidig så en at det kunne være krevende å ha overblikk over samspillet mellom de ulike lovbestemmelsene som gir rett til innsyn. Derfor ble det etablert en plikt for behandlingsansvarlige til av eget tiltak å veilede om retten til å be om lovbestemt innsyn. Forutsetningen er at lovbestemt rett til innsyn gir tilgang til flere opplysninger enn etter personopplysningsloven.[48]

Personopplysningsloven vil nesten alltid innebære at parten har rett til å få innsyn i flere personopplysninger enn etter forvaltningsloven.[49] Dette innebærer at forvaltningsorganer nesten alltid vil ha veiledningsplikt i forhold til lovbestemt innsyn i samsvar med pol § 6 annet ledd. Bestemmelsen er imidlertid neppe godt kjent i forvaltningen, og har derfor trolig en beskjeden praktisk betydning. Riktignok skal forvaltningsorganer uansett av eget tiltak vurdere partenes behov for veiledning, og herunder veilede om regler for saksbehandlingen,

48 Se pol § 6 annet ledd.

49 Årsaken er at pol § 18 første ledd gir innsyn i generelle opplysninger, § 18 annet ledd gir rett til innsyn i personopplysninger som ikke er direkte knyttet til enkeltvedtaket, og § 18 tredje ledd gir rett til innsyn i utdypende opplysninger i samsvar med den registrertes konkrete behov.

særlig forvaltningslovens regler.[50] Bestemmelsen kan tolkes slik at denne delen av veiledningsplikten også omfatter veiledning om retten til innsyn etter pol § 18, men det er neppe realistisk at slik veiledning faktisk skjer særlig ofte. Dersom innholdet i pol § 6 annet ledd vedrørende veiledning om lovbestemt innsyn hadde kommet direkte til uttrykk i forvaltningsloven, ville muligheten for etterlevelse være langt større. Også på dette punktet er dagens forhold mellom forvaltningsloven og personopplysningsloven for utydelig.

5. Hvem skal føre tilsyn med den elektroniske forvaltningen?

Datatilsynet og klageinstansen Personvernnemnda er eksempler på uavhengige forvaltningsorganer som bare er underlagt regjeringen («Kongen») og vedkommende departement i administrative spørsmål.[51] Andre eksempler på en slik uavhengig stilling i norsk forvaltning er Likestillings- og diskrimineringsombudet[52] og Partilovnemnda.[53] Felles for slike forvaltningsorganer er at de utøver offentligrettslig myndighet uten å kunne instrueres. Den nærmere kompetansen slike myndigheter kan ha varierer, men Datatilsynet er eksempel på en myndighet med meget bred kompetanse, noe som innebærer at tilsynet skal føre kontroll med etterlevelse av regelverket, treffe enkeltvedtak av ulike slag, og av eget tiltak gi uttalelser om spørsmål som vedrører personvern.[54] Datatilsynet har med andre ord en vid kompetanse som den kan anvende innenfor et meget vidt myndighetsområde, jf bestemmelsene om virkeområde i pol §§ 3 og 4.

Forvaltningsloven er plassert under et regime som er totalt forskjellig fra det som gjelder for personopplysningsloven. Til forvaltningsloven er det ikke opprettet noe særskilt tilsynsorgan, og loven bygger tvert i mot på at den skal håndheves gjennom den alminnelige adgangen til domstolsprøving og/eller behandling hos Stortingets ombudsmann for forvaltningen (Sivilombudsmannen).[55] Ombudsmannen har ingen vedtaksmyndighet, men kan si sin mening om en sak som er forelagt ham eller som han har tatt opp av eget tiltak.[56] Også Sivilombudsmannens arbeidsområde er vidt, og omfatter både generell og spesiell forvaltningslovgivning. Det innebærer at Sivilombudsmannen arbeider

50 Se fvl § 11 annet ledd bokstav b.
51 Se pol § 42 første ledd og § 43 første ledd.
52 Se diskrimineringsombudsloven av 10. juni 2005 nr. 40, § 2 annet ledd.
53 Se partiloven av 17. juni 2005 nr. 102, § 24 første ledd.
54 Se nærmere om Datatilsynets oppgaver i pol § 42 tredje ledd.
55 Ordningen med sivilombudsmannen ble opprettet i 1962, se lov av 22. juni 1962 nr. 8.
56 Se sivilombudsmannsloven § 10. Sivilombudsmannen kan også uttrykke sin mening overfor påtalemyndigheten om hva som bør foretas overfor tjenestemenn.

med den delen av lovgivningen som er berørt av aktuelle enkeltvedtak mv, samt de saker ombudsmannen tar opp etter eget initiativ. Forvaltningsloven inngår naturligvis som en viktig lov i dette arbeidet, men også personopplysningsloven inngår, fordi også denne loven regulerer vesentlige sider av forvaltningens virksomhet.[57]

I de foregående avsnittene i denne artikkelen har jeg vist hvorledes forvaltningsloven og personopplysningsloven ofte må ses i sammenheng for på den måten å få oversikt over den samlede rettslige reguleringen av forvaltningens behandling av personopplysninger. Myndighetssituasjonen ved håndhevelsen av de to lovene er ulik, avhengig av om en velger den ene eller andre loven som utgangspunkt. Datatilsynet kan selvsagt ta stilling til egen anvendelse av forvaltningslovens regler mv i saker som tilsynet behandler, men har ikke myndighet til å treffe enkeltvedtak om at et forvaltningsorgan må legge en bestemt forståelse av forvaltningslovgivningen til grunn for sin myndighetsutøvelse, selv om spørsmålet gjelder behandling av personopplysninger. Datatilsynet kan med andre ord ikke på autorativ måte avgjøre den type spørsmål om alminnelige sammenhenger mellom personopplysningsloven og forvaltningsloven som jeg har drøftet i denne artikkelen. Når Datatilsynet treffer vedtak som vedrører offentlig forvaltning, er det med andre ord ut i fra personopplysningslovens bestemmelser.

I tillegg til kompetansen til å treffe vedtak i enkeltsaker, har Datatilsynet vid kompetanse til på ulike måter å involvere seg og uttale seg i saker som gjelder ivaretagelse av personvern. Denne delen av tilsynets oppgaver er ikke bare knyttet til personopplysningsloven og elektronisk behandling av personopplysninger mv, men gjelder ivaretakelse av personvern generelt. Kompetansen er heller ikke begrenset til eksisterende forhold, men gjelder også spørsmål om hvorledes for eksempel offentlig forvaltning skal innrette seg i fremtiden. Datatilsynets oppgaver og kompetanse kan dermed sies å utgjøre et sterkt utgangspunkt for å være en aktiv aktør i spørsmål om utforming og praksis av elektronisk forvaltning. I 2005 ble det således publisert 22 høringsuttalelser på tilsynets nettsider, hvorav et stort antall var relatert til offentlig forvaltning.

Sivilombudsmannen kan også ta opp saker av eget tiltak, og har fra 2005 tatt opp flere slike saker enn tidligere.[58] Nevnte saker er imidlertid forholdsvis konkrete og har i liten grad det klare rettspolitiske preget slik saker Datatilsynet tar opp ofte har. Sivilombudsmannen er også høringsinstans i en

57 Det er imidlertid tegn på at personopplysningsloven sjelden blir anvendt av Sivilombudsmannen. Ved søk på hele Sivilombudsmannens nettsted den 6. juni 2006, var det kun én forekomst av ordet «personopplysningslov», og det var i en sak der ombudsmannen gjorde oppmerksom på at forholdet til denne loven ikke var undersøkt (sak 2005/73).

58 64 saker i 2005 mot 18 saker i 2004.

rekke spørsmål, men avgir forholdsvis få uttalelser, og er ikke spesielt opptatt av IKT-relaterte spørsmål slik Datatilsynet er. Uten å ha gjort en systematisk sammenligning av uttalelsene fra ombudsmannen og Datatilsynet, er inntrykket at Sivilombudsmannen er langt mer forsiktig i sine uttalelser enn det Datatilsynet er. Datatilsynet kan dessuten gi uttrykk for syn på forholdsvis konkrete spørsmål vedrørende innretningen av informasjonssystemer mv, mens inntrykket er at Sivilombudsmannen gjør dette i langt mindre grad.

Datatilsynets og Sivilombudsmannens ulike myndighet og rolle innen henholdsvis personvern- og rettssikkerhetsspørsmål, gir etter min mening mulighet for to betydningsfulle effekter. For det første kan Datatilsynets avgjørelsesmyndighet, brede mandat og høye medieprofil gjøre at et forholdsvis stort antall av de rettsspørsmål som reises i debatten om den elektroniske forvaltningen er personvernspørsmål. Inntrykket er at eforvaltning primært har blitt rettslig analysert ut i fra synsvinkelen personvern.[59] For det andre kan oppmerksomheten om og vektleggingen av personvernspørsmål, gjøre at flere spørsmål defineres som personvernspørsmål. Forholdsvis vide formuleringer i personvernteori og lovgivning, kan leses i denne retningen. «Krav om begrunnelse» og flere krav under «interessen i brukervennlig behandling» i den norske teorien om personverninteresser, har (også) åpenbare rettsikkerhetsmessige begrunnelser. Det samme kan sies om lovbestemmelser vedrørende informasjon/begrunnelse for helt automatiserte avgjørelser (pol § 22) og rett til avgjørelser som er basert på manuell behandling (pol § 25). En utvidet forståelse av personvernbegrepet kan uansett sies å være en mulig strategi for at spørsmål vedrørende eforvaltningen kan komme inn under en aktiv og kompetent myndighet.

På den ene side kan en se disse (mulige) utviklingstrekkene som Datatilsynets fortjeneste. Samtidig skaper det en ubalanse i forholdet til de rent rettssikkerhetsmessige og forvaltningsrettslige perspektivene på elektronisk forvaltning. Det kan selvsagt ikke Datatilsynet kritiseres for; og heller ikke Sivilombudsmannen som har en annen rolle å spille enn å delta i den aktive politikkutformingen. Asymmetrien oppstår i første rekke fordi det mangler et tilsynsorgan tilsvarende Datatilsynet på rettssikkerhetens område.

En lettvint løsning er å stille forslag om et nytt tilsyn; og det kan etter min mening ikke helt avvises at tilsynsstrukturen og ombudsmannsordninger bør revurderes, men jeg avstår fra å diskutere denne spørsmålsstillingen her. Uansett ligger det imidlertid muligheter for en mer balansert rettslig analyse

59 Et søk på regjeringens web-server Odin.no gir en indikasjon på at dette inntrykket kan være riktig. Søk på «elektronisk forvaltning» og beslektede uttrykk sammen med henholdsvis «personvern» og «rettssikkerhet», gav 15 treff på kombinasjonen med personvern og kun 4 treff med kombinasjonen rettssikkerhet.

av eforvaltningen dersom regjeringsapparatet *selv* ble mer bevisst slike spørsmål og dyktiggjorde seg innen rettslige problemstillinger som oppstår i møte mellom IKT og ivaretakelse av rettssikkerhet. Samtidig må oppmerksomheten rettes mot sammenhengen mellom rettsikkerhets- og personvernspørsmål, jf foranstående avsnitt i denne artikkelen. En slik strategi er imidlertid tung å realisere fordi det lovgivningsmessige grunnlaget for å se sammenhenger mangler. Det er derfor et behov for å se nærmere på relevant lovgivning.

6. Personvern, eForvaltning og lovreform

I kapittel 17 i denne boken diskuterer Erik Boe behovet for å revidere forvaltningslovgivningen, sett i lys av automatisering av beslutninger og generell bruk av IKT i forvaltningen. Her skal jeg derfor la dette generelle spørsmålet ligge. Et delspørsmål gjelder imidlertid forholdet mellom forvaltningsloven og personopplysningsloven, nærmere bestemt om det bør skje lovendringer som gjør det lettere å se sammenhengen i de to regelsettene. Etter min mening taler meget for å endre forvaltningsloven for at slike sammenhenger skal komme klart frem. En lovendring bør etter min mening primært skje i forvaltningsloven, dvs i den loven som saksbehandlere og andre ansatte i forvaltningsorganer er opplært til å følge. Målsettingen bør være å gjøre endringer som gjennomfører personverndirektivet på de punkter der det er intim sammenheng mellom forvaltningsloven og personopplysningsloven. Dette gjelder i det minste på punkter der bestemmelser i begge lover i dag må anvendes for å gjennomføre regulær enkeltsaksbehandling, jf de fleste problemstillinger som er reist i denne artikkelen. En innarbeidelse av bestemmelser som gjelder behandling av personopplysninger innenfor rammene av forvaltningens enkeltsaksbehandling, bør ikke skje ved en transskribering av personopplysningslovens bestemmelser. Målsettingen må i stedet være å formulere bestemmelser i forvaltningsloven som harmonerer med denne lovens øvrige bestemmelser, samtidig som en sikrer full gjennomføring av personverndirektivet.

Dersom en skulle velge å innarbeide bestemmelser vedrørende behandling av personopplysninger i forvaltningsloven, vil det stille lovgiver overfor viktige regulatoriske valg. Dette gjelder særlig valget mellom en individuell og systemmessig tilnærming til forvaltningens saksbehandling. Skillet mellom «individ» og «system» kan dels anvendes på myndighetssiden, og dels for parter. Valget kan med andre ord stå mellom bestemmelser som fastsetter i hvilken grad myndigheter skal forholde seg til individuelle, konkrete saker og i hvilken grad de skal forholde seg til informasjons-/saksbehandlingssystemet, dvs på et generelt/semi-generelt nivå. Tilsvarende kan vi velge i hvilken grad parter skal forholde seg til (deres) individuelle saker og i hvilken grad de kan forholde

seg til systemet for saks- og informasjonsbehandling som sådan. Her har jeg ikke mulighet for å ta opp spørsmålet i sin fulle bredde, men vil avslutningsvis antyde noen problemstillinger og mulige implikasjoner.

Som jeg tidligere har påpekt er forvaltningsloven individuelt orientert på myndighetssiden, dvs den forutsetter at forvaltningsorganer foretar konkrete vurderinger av individuelle forhold. Innen personopplysningsloven kan «behandlingsansvarlig» være en forvaltningsmyndighet. På myndighetssiden er denne loven langt mer systemorientert, dvs. den stiller i stor grad krav til hvorledes informasjonssystemer som behandler personopplysninger skal være, jf særlig pol §§ 13 (informasjonssikkerhet) og 14 (internkontroll). Mange andre bestemmelser stiller primært krav til system, selv om de også har viktige funksjoner i forhold til individuelle saker. Således er den viktigste effekten av krav til rettslige grunnlag for å behandle personopplysninger (pol §§ 8 og 9) at det må skje en *gjennomgående* vurdering av mulige lovhjemler, krav til samtykke mv; som ledd i planleggingen av det aktuelle informasjonssystemet. Samtidig har bestemmelsene selvsagt den funksjon at de kan danne grunnlag for avgjørelser i konkrete saker, for eksempel fordi nødvendig samtykke mangler. Poenget her er at lovgiver i møte mellom forvaltningsloven og personopplysningsloven vil stå overfor spørsmålet om i hvilken grad berørte (nye) bestemmelser i forvaltningsloven i større grad enn i dag skal være systemorienterte.

	Individuelt orientert	Systemorientert
Myndighet	Fvl	Pol
Part	Pol, fvl	Ny regulering?

Graden av systemorientering gjelder som nevnt både myndighetssiden og i relasjon til partene. Forvaltningsloven og personopplysningsloven er i dag individuelt orientert når det gjelder reguleringen av parters forhold, og hovedtilnærmingen er å gi individuelle rettigheter, dvs rettigheter som (direkte) kun har effekt for parten selv. En systemorientering av parters rettigheter er imidlertid mulig, og etter min mening også logisk innen den elektroniske forvaltningen. En individuell klage og omgjøring av et vedtak som er truffet av et beslutningssystem med automatisert saksbehandling gir – som flere har påpekt – kun begrenset mening.[60] Selv om uriktige enkeltvedtak blir endret, har det meget begrenset effekt så lenge beslutningssystemet som produserte feilen er uendret. Denne situasjonen er derfor eksempel på at det som i dag er en individuell rett for parten (til å klage), kanskje også bør omfattes av forpliktelser for forvaltningsorganet til

60 Om klage på automatisk fattede vedtak, se Bing 1977.

å se på de systemmessige implikasjonene av den feilen som eventuelt avdekkes. Tilsvarende kan tenkes på en rekke andre problemområder, dvs i prinsippet kan enhver berettiget kritikk fra parter i den elektroniske forvaltningen begrunne vurderinger og endringer av systemmessig art. Dermed er det imidlertid ikke sagt at dette bestandig skal skje på grunnlag av lovbestemmelser som gir individuelle rettigheter. Også plikt til å forfølge mulige systemimplikasjoner av klager fra parter, innenfor rammene av lovens krav til forvaltningens internkontroll (jf pol § 14), er en mulighet.[61]

Diskusjonen om systemorientering av lovgivningen peker i retning av en større debatt enn den jeg her har forholdt meg til; nemlig spørsmålet om behovet for en bred gjennomgang av forvaltningsloven ut i fra det faktum at forvaltningen i stadig større grad blir elektronisk og – i stor grad – automatisert. E-forvaltning og automatisering av forvaltningens enkeltvedtak handler nettopp om å bygge informasjonssystemer – og da er det nærliggende å anta at også forvaltningslovgivningen i større grad bør være systemorientert.

Litteratur

Bing 1977, Jon Bing: Automatiseringsvennlig lovgivning, I: Tidsskrift for Rettsvitenskap 1977 (s 195 – 229).

Bygrave 2002, Lee A Bygrave: Data Protection Law. Approaching Its Rationale, Logic and Limits, Kluwer 2002.

Graver 2002, Hans Petter Graver: Alminnelig forvaltningsrett, Universitetsforlaget 2002.

Schartum 2001, Systemrettssikkerhet, I: Rättsinformation under 2000-talet. Nuläget i Sverige och Europa, trender och policy 2000, SOU 2001: 71.

Schartum og Bygrave 2004, Dag Wiese Schartum og Lee A Bygrave: Personvern i informasjonssamfunnet, Fagbokforlaget 2004.

Woxholth 1999, Geir Woxholth: Forvaltningsloven med kommentarer, adNotam Gyldendal 1999.

61 En nærmere gjennomgang av mulige nye rettssikkerhetstiltak knyttet til IKT-systemer i offentlig forvaltning, finnes i Schartum 2001.

FRA SKATT MED HULLKORT TIL STUDIELÅN VIA SMS*

IKT SOM ET REDSKAP FOR AUTOMATISERING ELLER DRIVKRAFT FOR ENDRING

Arild Jansen

Abstrakt

Denne artikkelen diskuterer utviklingen av statens IKT-politikk i et historisk perspektiv, og ser på forholdet mellom den generelle forvaltningspolitikken og framveksten av IKT-politikken. Vi har sett en utvikling fra å betrakte IKT som et verktøy for rasjonalisering og effektivisering til at IKT i dag utgjør en integrert del av forvaltningen på alle nivåer. Spørsmålet som drøftes er i hvilken grad den norsk forvaltningens spesifikke karakter har preget IKT-politikken, eller om dynamikken i teknologiutviklingen har gjort det nødvendig å styre ut i fra andre hensyn?

Analysen synes å vise at de grunnleggende prinsippene i norsk forvaltning ligger fast; det enkelte forvaltningsorgans sjølstendige ansvar og myndighet for egen oppgaveløsning og det kommunale sjølstyret er ikke endret som følge av IKT-utviklingen. Men framveksten av interorganisatoriske systemer og tverrsektorielle løsninger sammen med en omfattende datautveksling mellom stat og kommune utfordrer dette i økende grad.

Nøkkelord: *Statens IKT-politikk, forvaltningspolitikk, samordning,*

1. Innledning

Da Holkortsentralen på Vestlandet, i samarbeid med Universitetet i Bergen og flere sentrale Bergens-bedrifter i 1957 gikk til anskaffelse av IBM-maskinen

* Også publisert i Habib (red) Proceedings fra NOKOBIT2007, Holmenkollen Park 21-22.11.2007

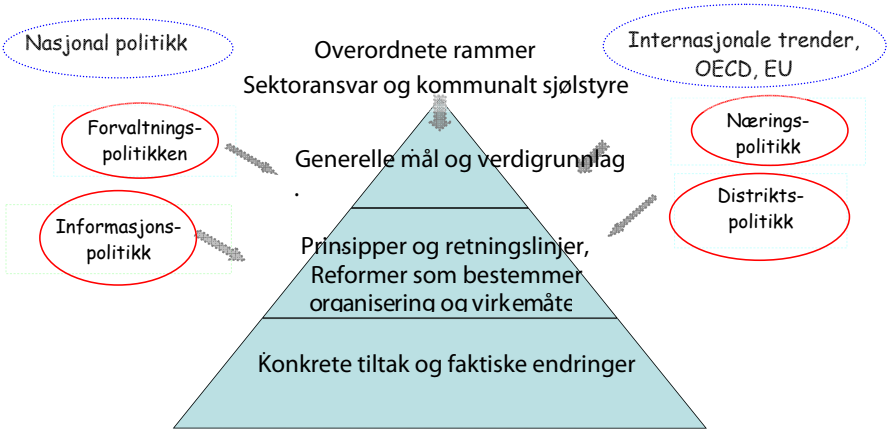
650 (også kalt EMMA) til å beregne skatt av årets ligning, var dette ikke som et ledd i en gryende statlig datapolitikk. Finansdepartementet var midt sagt skeptisk til at staten skulle betale universitetets leiekostnader, på tross av at Kirke- og undervisningsdepartementet hadde støttet opp under prosjektet. Dette på bakgrunn av at Statens Rasjonaliseringsdirektorat hadde konstatert at «de opplysninger som er lagt fram for Rasjonaliseringsdirektoratet gir ikke tilstrekkelig grunnlag for en vurdering av lønnsomheten av de utgifter det her er snakk om» Haraldsen (2003:42). Finansdepartementet mente at saken burde utstå til den var vurdert av det påtenkte utvalget for samordning av statens bruk av elektroniske maskiner[1]. Kan vi likevel si at dette var et naturlig resultat av økt fokus på rasjonalisering innen offentlig sektor, en rådende trend på 50-tallet, og derved i tråd med forvaltningspolitikken? Eller var dette snarere et første skritt i retning av modernisering av offentlig sektor, hvor teknologiutviklingen var et sentralt element?

Temaet for dette kapitlet er nettopp forholdet mellom den generelle forvaltningspolitikken og framveksten av en etter hvert identifiserbar data- eller IKT-politikk. Vi vil forsøke å finne de overordnede linjene gjennom å se i hvilken grad den norske forvaltningens særpreg og historiske tradisjoner har styrt IKT-politikken, men samtidig prøve å avdekke hvordan IKT-utviklingen har påvirket den generelle forvaltningspolitikken.

Vi antar at mange ulike eksterne forhold påvirket IKT-politikken, både internasjonale trender, teknologiutviklingen, mer globale markeder og reguleringsregimer, næringslivets påvirkning, borgernes forventninger med mer. Som en analytisk modell vil vi forsøke å plassere IKT-politikken innenfor dette rammeverket[2]:
Vi kan da formulere våre generelle hypoteser slik:

i. IKT har i hovedsak vært anvendt som et redskap med sikte på å nå de generelle målene i forvaltningspolitikken (verktøyperspektivet)
ii. Utvikling, innføring og bruk av IKT har utgjort en betydelig drivkraft og premissgiver for utviklingen av forvaltningspolitikken (teknologiperspektivet)

1 Finansdepartementet opprettet i 1957 et utvalg for å utrede edb-behovet i staten
2 I denne artikkelen vil vi i hovedsak begrense oss til å se på forholdet mellom den generelle forvaltningspolitikkens og IKT-politikken, men hele studien vil trekke inn andre relevante politikkområder



Figur 1 Rammer for IKT-politikken

Utgangspunkt for den første hypotesen er å forstå IKT som et verktøy, og å undersøke i hvilken grad forvaltningen har tatt dette i bruk innenfor rammene av den generelle forvaltningspolitikken. Teknologien blir i følge dette perspektivet betraktet som et styrbart redskap i den forvaltningspolitiske verktøykasse, på linje med juridiske, økonomiske, organisatoriske eller andre virkemidler. Vi antar at teknologien er tatt i bruk ut i fra veldefinerte målsetninger, basert på beslutninger som følger den parlamentariske styringskjeden. Teoretisk kan dette perspektivet forankres i et instrumentelt-hierarkisk perspektiv, som antar at forvaltningen styres ut i fra formelle og rasjonelle beslutninger for å fastsette mål og bruk av virkemidler, og at hvert forvaltningsorgan har sin spesifikke kompetanse og beslutningsmyndighet (se f eks. Christensen og Egeberg 1997, Christensen et al. 2004). I dette perspektivet er det viktig å klarlegge de fastsatte mål og virkemidler og på hvilket nivå beslutningene er fattet (av Stortinget, av fagdepartement, i etatsledelse osv.), og om den parlamentariske styringskjeden synes å ha fungert.

Den andre hypotesen baserer seg på en forståelse av teknologien som en sjølstendig drivkraft for endringer i forvaltningen, og hvor vi ønsker å se hvordan denne forståelsen faktisk har påvirket beslutningsprosessene i forvaltningen og bidratt til at andre hensyn er blitt lagt til grunn. Flere teoretiske perspektiver kan begrunne en slik forståelse, f eks. organisasjonsendring som resultat av forhandlinger (Christensen 2004, Aberbach og Christensen 2005:3). Alternativt kan en legge vekt på påvirkning fra omgivelsen, ved at en antar at offentlige organisasjoner må tilpasse sine interne forhold til omgivelsene for å utvikle seg og være effektiv, som vektlegges i blant annet i

betingelsesteoriene (contigency-teoriene) (Andersen og Abrahamsson 1996: 84, Nylehn (1997:190)). En viktig påvirkningsfaktor fra omgivelsene vil i denne sammenheng være teknologiutviklingen, og de krav til styring og organisering denne skaper, og som målbæres av ulike grupper interessenter og aktører. På et overordnet nivå i analysen vil dette kreve identifikasjon av motiver og interesser, mens det på et mer detaljert nivå vil være å klarlegge bruk av ulike virkemidler, som valg mellom ulike organisasjonsmodeller, standardisering og fellesløsninger osv. Det gjelder således å klarlegge om hensynet til teknologien har hatt innflytelse for utforming av forvaltningspolitikken, og i så fall på hvilken måte.

Forskningsdesign og metodisk tilnærming

Denne studien bygger på en deduktiv forskningsstrategi, basert på en kvalitativ tilnærming hvor formålet er å avdekke om mål og virkemidler i IKT-politikken faktisk har vært i tråd med den rådende forvaltningspolitikken. Konkret vil dette innebære å avdekke i hvilken grad krav fra «edb-miljøene» om konkete IKT-tiltak, f.eks. nye systemløsninger, bedre samordningstiltak osv. har hatt innflytelse på den generelle forvaltningspolitikken. Vi må da studere om det er samsvar mellom både overordnete målsetninger og de ulike typer virkemidler som er blitt anvendt. Vi vil i analysen anvende dette enkle analyseskjemaet.

		Forvaltningspolitikken		IKT-politikken	
		Visjon og mål	Virkemidler	Mål for IKT-bruken	Virkemidler
Tidsperioder			Samsvar eller avvik		

Tabell I: Skjema for sammenhengen mellom forvaltningspolitikken og IKT-politikken

Analysene i dette kapitlet baserer seg på studier av et utvalg sentrale dokumenter som beskriver rammene for forvaltningspolitikken i de aktuelle tidsperiodene, og sammenholder dette med IKT-politiske dokumenter som beskriver de generelle datapolitiske beslutningene[3]. I analysene har vi forsøkt å avdekke både hva slags mål som ble formulert (som. effektivisering, bedre tjenester, høyere kvalitet osv.), og hvilke virkemidler som faktisk ble anvendt. Det har

3 Den empiriske basis er hentet fra utvalgte NOU'er, St. meldinger og innstillinger med mer, videre noen budsjettdokumenter for utvalgte etater. Videre var undertegnede ansatt i Fad i perioden 1984-89 og arbeidet med datapolitiske spørsmål, blant annet som sekretær for NOU 1988:48.

vært særlig viktig å kartlegge hvilke konkrete mål og virkemidler som har hatt størst vekt gjennom de ulike perioder, og hvordan synet på IKT eventuelt har påvirket målformuleringer og virkemiddelbruk. Utfordringen er å identifisere hvilken rolle den faktiske teknologiforståelsen har spilt i beslutningsprosessene, og hvilke effekter vi kan se av dette i forhold til endringer i forvaltningspolitikken.

2. Litt om utviklingen av forvaltningspolitikken – stabilitet eller dynamikk?

Forvaltningspolitikken retter seg innover mot det administrative apparat, og skal bidra til å oppfylle Regjeringens mål og samtidig tilstrebe en mest mulig effektiv ressursutnyttelse[4].

To grunnleggende prinsipper karakteriserer den norske forvaltningens virkemåte:

i. Rollefordeling mellom departementene innenfor det forvaltningspolitiske området: Det enkelte fagdepartement har ansvar for å velge formålstjenlige styringsvirkemidler og organisering innenfor de felles lov- og regelverk som til enhver tid er fastsatt. Dette innebærer at den enkelte etat og institusjon, innenfor overordnete lovpålagte rammer og retningslinjer har sjølstendig ansvar og myndighet. Det framheves f. eks. i St.meld. 31(1975–76) at hovedmålet for effektiviseringstiltak i staten er «delegering og desentralisering av oppgaver og avgjørelser til regionale og lokale organer». Videre vektlegges at «på hvert sitt fagområde er direktoratene sentraladministrative organer med utøvende funksjoner, dvs. en sektorisering som innebærer de enkelte sektordepartementers og underliggende etater delegerte ansvar og myndighet.»

   Dersom en sammenligner den norske styringsstrukturen med andre land, ser man at den har mange likhetstrekk med Danmark, og står i motsetning til den britiske modellen hvor Statsministeren har større overordnet styring, og den svenske, hvor Regjeringens medlemmer har et kollektivt ansvar for beslutningen (Eriksen, 2001).

4 På Fornyings- og administrasjonsdepartementets nettside heter det blant annet: *Forvaltningen skal være et redskap for utøving av sektorpolitikk og tjenesteyting.[..]. Forvaltningspolitikken er et virkemiddel for å ivareta verdier som demokratisk politisk styring, rettssikkerhet i offentlig myndighetsutøvelse, effektiv ressursbruk og måloppnåelse[..] . Forvaltningspolitikken er tverrsektoriell ved at den gir allmenne retningslinjer for utformingen av forvaltningen på tvers av departementssektorer.*

ii. ii) Forholdet mellom statlig og kommunal forvaltning, forankret i det kommunale sjølstyre som ble etablert gjennom formannskapsloven av 14. januar 1837, gjeldende fra 1. januar 1838 og ført videre av Kommuneloven av 1993. Dette innebærer at statlige forvaltningsorganer ikke uten videre kan gripe direkte inn i kommunal forvaltning.

Disse prinsippene har imidlertid også blitt utfordret mange ganger, ikke minst knyttet til edb-utviklingen, og ble aktualisert allerede ved anskaffelsen av EMMA i 1957. Vi ser det også på andre områder, knyttet til f eks. felles infrastrukturer, videre sikkerhet og sårbarhet, hvor det framheves at viktige samfunnshensyn tilsier et overordnet ansvar og styring. Dette har, som vi skal se, hatt stor betydning for hvordan datapolitikken har vært utformet.

Selv om disse grunnleggende sidene ved hovedprinsippene og innretningen av forvaltningspolitikken har ligget fast, har det skjedd betydelige endringer i organiseringen og ikke minst når det gjelder rammene for den enkelte etat og virksomhet. Dels har det vært endringer som har «tvunget» seg fram fra indre spenninger og skiftende politiske regimer, dels er det resultat av påvirkning utenfra, ikke minst gjennom deltakelse i OECD-samarbeidet og etter hvert i EU' forskingssamarbeid. Nedenfor skal vi begrense oss til noen trekk som er særlig relevante for IKT-utviklingen og framveksten av en egen politikk for denne.

Framveksten av velferdssamfunnet

Veksten i forvaltningen, ikke minst framveksten av velferdsstaten førte etter hvert til en sterkere vektlegging av departementenes politiske og styrende funksjoner som skulle fungere som sekretariater for statsrådene, jf. f. eks. St.meld. 31(1975–76), mens direktorater og andre underliggende etater skulle være utøvende organer. Den første perioden etter krigen var hovedfokuset på rasjonalisering og effektivisering, noe som opprettelsen Statens rasjonaliseringsdirektorat[5] i 1947 under Finansdepartementet vitner om.

Ved opprettelse av Forbruker- og administrasjonsdepartementet (Fad) i 1972 ble det framhevet at det nye departementet skulle «arbeide kontinuerlig med den videre utvikling og effektvisering av statsadministrasjonen, herunder en langsiktig plan for administrativ utvikling i statsforvaltningen». Det kan også være verdt å merke seg at regjeringen i proposisjonen uttaler at «[dette nye] departementets arbeidsoppgaver, særlig på planleggings- og

5 Statens Rasjonaliseringsdirektoratet ble opprettet 1947. I 1962 opprettes Opplæringsseksjonen i Personaldirektoratet og i 1965 Statens informasjonstjeneste og System- og datagruppen.

utredningssiden, krever stor fleksibilitet med hensyn til organisasjon og personelldisponering». (St. prp. 85(1971–72).

Spørsmålet om samordning av effektiviseringsinnsatsen ble også drøftet i Innst.S. nr 72 (1973–74) hvor det heter: «Sjøl om det alltid vil være behov for å tilgodese behovet for samordning, må en være varsom med å binde opp forvaltningen med detaljert regelverk [..] Videre: Dette betyr at effektiviseringsarbeidet ikke kan overlates til spesielle effektiviseringsorganer, men i stor utstrekning drives som en prosess der i prinsippet alle tjenestemenn er med, hver ut i fra sin kompetanse.» Derimot er ikke bruk av edb som virkemiddel nevnt her, noe som drøftes nedenfor.

Modernisering av forvaltningen: brukerorientering, fornyelse og forenkling

Det var først fra begynnelsen av 80-tallet at forvaltningspolitikk egentlig ble anerkjent som et særskilt politikkområde, representert ved en egen enhet i daværende Fad. I motsetning til tidligere ble forvaltningsreformer på 1980-tallet lansert som *programmer* for hele statsforvaltningen (Statskonsult 2006). Dette ble innledet av Astrid Gjertsen i 1986 ved Moderniseringsprogrammet (Fad 1986), som markerte et tydelig brudd med rådende forvaltningspolitikken. Stikkord er her mål- og resultatstyring, brukerorientering og forenkling, friere rammer vedr. budsjett og økonomi, fristilling, og i noen grad privatisering. Her ser vi elementer av det som senere er blitt omtalt som New Public Management (NMP), karakterisert blant annet ved markedsorientering, deregulering og økt konkurranse (Christensen og Lægreid 2001). Senere har ulike norske regjeringer hatt tilsvarende programmer for fornyelse av offentlig sektor, da under ulike slagord om modernisering, forenkling og fornyelse. Det har vært ulike syn på hvilke formål som skal prioriteres og hvilke virkemidler som ansees hensiktsmessige, men likevel ikke dramatiske forskjeller.

Tidlig på 1990–tallet ble den forvaltningspolitiske tenkningen systematisert i St.meld. nr. 35 (1991–92). På flere måter var dette en videreføring av den gjeldende politikken, men enkelte sentrale premisser ble modifisert. Organisasjons- og styringsformene i offentlig virksomhet var et viktig tema i meldingen, basert på NOU 1989:5 *En bedre organisert stat*, som blir fulgt opp i denne stortingsmeldingen. Endringene i statens budsjettsystem fikk Stortingets tilslutning i 1990 og 1991, noe som innebar friere rammebetingelser for offentlige virksomheter. Det slås blant annet fast at staten bør i hovedsak organisere virksomheten som statlige forvaltningsorganer, og det advares mot å blande forvaltningsmessig myndighetsutøvelse og forretningsmessig yting av monopoltjenester på samme virksomhetsområde. Dette la grunnlaget for fristilling eller utskilling av forretningsmessige virksomheter som Televerket til Telenor og Kartverket til Statskart, osv.

De senere programmer, som f.eks. Det Norske Hus[6] (1996–1997) markerte et brudd med NPM-påvirkningen ved å orientere seg mer mot en Governancetenkning basert på kunnskapsoppbygging og politikkutvikling på tvers av sektorer og hierarkier, mens etterfølgeren *Et enklere Norge* (1999) var derimot preget av forenkling og brukerorientering i forhold til kommunene, næringslivet og borgerne. Dette preget også Moderniseringsprogrammet (2002), som igjen hadde hovedfokus på delegering, desentralisering og brukerorientering, blant annet med å omfatte et program for utflytting av statsetater, og ellers særlig fokus på markedstenking, konkurranseutsetting og delprivatisering. Statskonsult ble omdannet til et heleid statlig aksjeselskap fra 1. januar 2004, som mange mener reduserte regjeringens kapasitet innen forvaltingspolitikken, og spesielt på det IKT-politiske området[7].

Teknologien spilte i de første programmene en relativt beskjeden rolle, hvor elementer i relasjon til IKT-politikken var blant annet økt brukerfokus, nye finansieringsformer, endrede konkurransevilkår (f.eks. åpen konkurranse om IKT-tjenester som fellessystemer, nye styringsformer, omorganisering m.m.). Ut på 90-tallet og etter at Internett fikk sitt gjennombrudd, begynte IKT å spille en mer framtredende rolle som pådriver, blant annet i sektorplanen for IKT 1992–1995. Dette er svært tydelig i Bit-for-Bit-rapporten, og i de senere planer.

En viktig reform er knyttet til etableringen av KOSTRA (Kommune-Stat-Rapportering), som er et rapporteringssystem basert på elektronisk informasjonsutveksling mellom stat og kommune (Fimreite 2006). KOSTRA kan imidlertid oppfattes som et statlig styringssystem, gjennom å legge data produsert gjennom KOSTRA til grunn for ulike tiltak overfor kommunene, f.eks. å redusere uønsket ulikhet i kommunenes velferdsproduksjon. Men kommunene har også nytte av aggregert informasjon som sendes tilbake, og derved kan brukes i kommunenes egen økonomistyring. Det er datateknologien som har gjort dette mulig, og systemet illustrerer at et IKT-system kan brukes på flere måter og ha ulike virkninger, i dette tilfelle f.eks. som et hinder eller som verktøy for lokaldemokratiet.

6 Av Jagland-regjeringen med Bendik Rugaas som leder av Planleggings- og samordningsdepartementet

7 Det er derfor interessant å merke seg at regjeringen fra 1.1.2008 oppretter Direktoratet for forvaltning og IKT, som en sammenslåing av Statskonsult AS, Norge.no og E-handelssekretariatet.

Oppsummering: fra rasjonalisering til markedsstyring?

Vi har sett at mens forvaltningspolitikken de første 10-årene etter krigen i stor grad hadde et innadrettet fokus og handlet primært om effektiv ressursutnyttelse (rasjonalisering), fikk vi fra 80-tallet en mer bevisst, utadrettet politikk, med vekt på *brukerretting av tjenestene, forenkling og tilgjengeliggjøring av tjenester*, *desentralisering, delegering og fristilling*, dog i ulik grad av skiftende regjeringer. Fad spiller en stadig viktigere rolle, men fortsatt har Finansdepartementet ansvar for budsjett- og økonomistyringen, slik at en i realiteten har to departementer med ansvar for dette politikkområdet, med sistnevnte som det mektigste. Fad har aldri blitt noe overordnet departement i Norge på linje med Finansdepartementet. På IT-området ser vi imidlertid at Fad etter hvert blir det sentrale departement.

	Forvaltningspolitikken	
	Visjon og mål	Virkemidler
1955–1970	Framvekst av velferdsstaten	Kostnadseffektivitet rasjonalisering
1970–1985	Videreutvikle velferdsstaten	Delegering og desentralisering
1985–1995	Brukerorientering, forenkling og begrense vekst	Målstyring, fristilling og økt konkurranse
1995–2005	Sikre rettigheter og økt valgfrihet	Økt tilgjengelighet og tjenestekvalitet

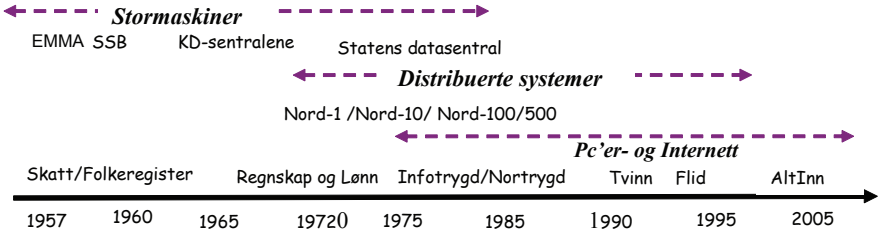
Tabell 2: Mål og virkemidler i forvaltningspolitikken

3. Framveksten av IKT-politikken

Som innledningen antyder, kan vi regne anskaffelsen av Emma i 1957 som starten på den norske edb-æraen, i alle fall når det gjelder forvaltningens bruk av datamaskiner. Og faktisk fikk dette datapolitiske konsekvenser, ved at det som nevnt ble oppnevnt et utvalg for å se på behovet for datakraft. Vi kan kanskje si at staten opplevde å bli «tatt på senga» av de framsynte og initiativrike ligningssjefer m.fl. på Vestlandet, men kom altså raskt etter gjennom anskaffelsen av en datamaskin til Statisk sentralbyrå i 1958.

Denne striden mellom ligningssjefene på Vestlandet og staten illustrerer også den konfliktlinjen som har ridd norsk datapolitikk i 50 år; ønsket om sentral kontroll og styring på den ene siden i forhold til lokale ildsjeler (innovatører) på den annen side som ser nye muligheter i den pågående teknologiutviklingen, og derfor ønsker å utnytte dette lokalt i egen organisasjon. Konfliktene

har omhandlet anskaffelser av datakraft, felles maskinteknisk[e] plattform[er], spørsmål om utvikling og bruk av felles programsystemer, felles dataregistre, samordning og standardisering, rammeavtaler med mer. Den datatekniske utviklingen fra tidlig 50-tall til i dag innebærer så vel teknologiske som organisatoriske og bruksmessige revolusjoner. En kort illustrasjon av noen hovedtrekk ved teknologiutviklingen i norsk forvaltning[8]:



Figur 2 Noen hovedtrekk ved den IKT- utviklingen i forvaltningen

Fellessystemer, sektorsystemer og etatsløsninger

Utviklingen av programsystemer i forvaltningen har vært konsentrert om applikasjonssystemer som skal løse bestemte oppgaver. En har gjerne gjort et skille mellom *fellessystemer og fagsystemer (sektorsystemer og institusjonssystemer)*. Fellessystemer som igjen kan inndeles i *funksjonelle systemer* som tar seg av fellesartede rutiner for hele forvaltningen[9], (økonomi, lønn, arkiv, osv), *og grunnlagssystemer*, som lagrer og behandler opplysninger som brukes innen mange områder, som Folkeregisteret, Arbeidsgiver-/Arbeidstagerregister, eiendomsregister, osv. Det som karakteriserer begge disse typer systemer er at de er basert på et felles regelverk som gjelder for alle forvaltningsorganer, i motsetning til sektor- og institusjonssystemene, som er basert på særlovgivning. Det var derfor gode grunner for å utvikle sentrale løsninger for disse funksjonene, og dette arbeidet startet på slutten av 60-tallet.

8 Utbredelsen av stormaskinene i USA på 50–tallet, i Norge fra 1958, innebar framveksten av store datasentraler og edb-avdelinger og tilhørende proprietære løsninger. IBM dominerte på 60- og 70-tallet, da både på statlig og kommunal side. Fra midt på 70-tallet fikk minimaskiner innpass, og etter hvert spesielt de norskproduserte ND-maskinene. Dette innebar også etter hvert en maktforskyvning fra datasentralene til avdelingene.

9 Viktige fellessystemer har vært Statens lønns- og personal system (SLP) og Det sentrale Økonomisystem (DØS), som begge er utviklet av R-direktoratet og ble kjørt på SDS og videre NOARK (NoU 1978:48 s56)

Av særlig interesse er også diskusjonene rundt utvikling, drift og bruk av funksjonelle fellessystemer som for økonomi, lønn og personal og etter hvert arkiv. Disse ble utviklet av SD-gruppa R-direktoratet, og ble etter hvert overført til Statens Datasentral. mens drift- og vedlikeholdsansvaret lå i R-direktoratet. Systemene ble imidlertid av mange oppfattet som påtvungne monopolsystemer, og at det brøt med prinsippet om etatenes sjølstendige ansvar for å planlegge, og anvende /ta i bruk egnet edb-løsninger for sin virksomhet. Det var således et press fra to kanter: internt i forvaltningen som opplevde fellesystemene som rigide og dyre i drift, og fra bransjen som mente at disse forhindret en åpen konkurranse. Etter en lang prosess ble det laget et opplegg for godkjenning, og etter hvert egne kravspesifikasjoner som skulle bidra til konkurranse i et åpent marked. I dag finnes det fastlagte kravspesifikasjoner for disse funksjonerområdene, og et antall konkurrerende leverandører i markedet[10], som også er i tråd med gjeldende forvaltningspolitikk.

Forvaltningspolitikkens innvirkning på IKT-politikken

1957 EMMA anskaffes. Beregner skatt fra 1958 – 63
1957 Finansdep. oppretter utvalg for å utrede EDB-behov i staten
1958 Første EDB-maskin i staten til Statistisk sentralbyrå
1961 Rådet for databehandling i staten etablert. Nedlagt 1979
1964 Innføring av 11-sifret personnummer. Forvaltes av Skatteetaten
1970 Kontaktutvalg mellom kommunal og statlige EDB-brukere
1967 Forvaltningsloven og Lov om offentlighet i forvaltningen (1970)
1972 Statens datasentral blir etablert
1976 Verdens første "Dataavtale" mellom partene i arbeidslivet
1978 NoU 1978:48 Desentralisering og effektivisering av off. db
1980 Lov om personregistre trådte i kraft
1981 Etablering av Løsøreregistret i Brønnøysund (BRREG)
1982 St. mld. 12 (1982-83) som behandler NoU 1978:48
1978:48. Opprettelse av datapolitisk råd
1991 Kgl. res om OSI-standarder
1993 Internet kommersielt tilgjengelig i Norge
1993-95 KD-sentrale/NIT og solgt til hhv IBM og Posten/Ergo group
1996 Den Norske IT-veien: Bit-for Bit blir lagt fram
2003 AltInn etablert og Lånekassens Nettsøknad kom på lufta
2006 MinSide ble satt i prøverdrift

Figur 3 Viktige datapolitiske begivenheter i forvaltningen

Spørsmål knyttet til edb-bruk var som vi har sett, ikke noe eget tema i forvaltningspolitikken på 60-tallet, eller ved opprettelsen av Fad i 1972. De årlige

10 Det er interessant her å merke seg at to at de største private aktørene er «restene» av de tidligere så «mektige» Statens datasentral og KD-sentralene, nå i hhv ErgoGroup og IBM.

rapporter fra R-direktoratet og Statens datasentral ble debattert i Stortinget som en del av effektiviseringsarbeidet, og anskaffelser m.m. var i hovedsak en del av den ordinære budsjettprosessen.

Først i St.meld. 37(1974–75) *Om planlegging av databehandlingen i forvaltningen*, det første datapolitiske dokument fra Fad, ble dette et eget tema. Meldingen er basert på NOU 1973:43 med samme navn, utarbeidet av Rådet for databehandling i staten. I meldingen drøfter departementet blant annet behovet for bedre samordning av arbeidet med planlegging og utvikling av edb-systemer, og spesielt forslag om en felles begreps- og systemstruktur og planleggingssystem. Mens utredningen foreslår et sentralt planleggingssystem for edb-sektoren, vektlegger departementet at «ansvaret for administrativt utviklingsarbeid påligger primært den enkelte institusjon. Det bør derfor ikke gjennomføres sentrale, overordnede ordninger når det gjelder organisering av databehandlingen som medfører vesentlige endringer i dette forhold. Databeh andlingsfunksjonene må vurderes som hjelpefunksjoner som det ikke kan være naturlig å ha en for sterkt sentralisert planlegging for.»

Likeledes heter det i administrasjonskomiteens innstilling[11]: «det er ikke tilstrekkelig grunnlag for en beslutning om oppbygging av en integrert systemstruktur i forvaltningen. [..] Utviklingen i retning av større samordning må først og fremst skje gjennom løpende praktisk samarbeid og kontakt mellom de enkelte departementer og institusjoner. [..] EDB er en av flere virkemidler i realiseringen av statsforvaltningens mål, og det er viktig at utviklingen på datafeltet blir tilpasset andre utviklingstiltak av organisatorisk, systematisk og personal-administrativ art.» Utsagnet illustrerer på en treffende måte noen av de spørsmålene som det har vært mest strid om i statens IKT-bruk.

Forvaltningspolitikken ble nok for alvor utfordret gjennom en ny utredning; NOU 1978:48, *Offentlig databehandling, Desentralisering og effektivisering* (også omtalt som Elgsaas-utredningen etter sin leder). Denne framstår nok som det mest grundige og omfattende dokument som er utarbeidet om IKT-politikken i forvaltningen, hvor det gis en detaljert oversikt over status og problemer i offentlig databehandling. I rapporten framheves disse målene for offentlig databehandling:

- Desentralisering av forvaltningens arbeidsoppgaver og beslutningsmyndighet
- Demokratisering gjennom å styrke og forvalte organers styring av IKT-bruken

11 Se Inst. S. fra nr. 256 (1974-1975) Inst. Fra adm. komiteen om planlegging av databehandling i staten

- Forenkling og effektivisering, og bedre forvaltningspublikumsservice

Vi vil her dvele litt ved denne utredningen og den oppfølgende i St.meld. 12(1982–193). Ikke bare fordi noen av beslutningene som ble tatt i 1982 fortsatt ligger til grunn for dagens politikk, men også fordi utredningen og meldingen berører mange grunnleggende spørsmål og dilemmaer i spenningen mellom forvaltningspolitikken og IKT-utviklingen, og som fortsatt er like aktuelle. Og ikke minst fordi resultatet av behandlingen la grunnlag for et «frislepp» i spredning av IKT i forvaltningen.

Hva stod striden om?

Utvalget peker på en rekke utfordringer knyttet til den sterkt økende bruk av edb i forvaltningen, som f.eks. «Den tekniske utviklingen har gått hurtig. Verken utdanningen av fagfolk eller den alminnelige forståelse av teknikkens muligheter, problemer og skyggesider har kunne holde tritt med den. Forsinkelser, fordyrelser og skuffelser over resultatene av EDB-prosjekter er ikke uvanlig.[..] Miljø-, sikkerhets- og sysselsettingsspørsmål dukker opp under marsjen. Egentlig unødvendig dobbeltarbeid påvises og manglende standardisering skaper vansker. Det etterlyses planlegging og forhåndsundersøkelser som skal fjerne enhver usikkerhet, og resultatvurderinger som skal bidra til at intet feilgrep blir gjentatt»

Dette var noe alle kunne slutte seg til. Men noen av de viktige, men kontroversielle forslagene var knyttet forslagene til at Fad skulle ha et overordnet ansvar for prinsipielle sider ved forvaltningens bruk av EDB, inkludert kommunenes virksomhet. Det foreslås opprettelse av regionale datautviklingsentra, sterkere vekt på samordning (sjøl om denne tenkes frivillig), videre utarbeidelse av systemkataloger og ulike typer oversikter, etc.

Utredningen skapte betydelig interesse og debatt, hvor en både finner sterk støtte for, og motstand mot, mange av forslagene. Spenningen og forventningene til Fad's behandling var således stor, både fordi mange av forslagene vil ha stor betydning for organisering av IKT-bruken. Men særlig fordi forslagene berørte forholdet mellom stat og kommune, og likeledes forholdet til ulike næringslivsinteresser, blant annet konkurransen mellom offentlige og private datasentraler og kompetansemiljøer.

«La de 1000 blomster blomstre»

Det ble Regjeringen Willoch, med Astrid Gjertsen (Forbruker- og administrasjonsminister og Petter Thomassen (Industriminister) som fremmet St.meld. 12(1982–83). Her ble flere av forslagene avvist, knyttet til etablering av blant annet ulike samordnende og koordinerende funksjoner. I meldingen framheves

det at datateknologien må oppfattes som et redskap, ikke som et virkemiddel i styringen av samfunnet: «Ansvar og myndighet vedrørende hjelpemidlene må følge ansvaret og myndigheten for hovedvirksomheten. Samarbeid er plikt når det er tydelig at dette gir besparinger eller enn effektiviseringsgevinst.» Som det framgår av oversikten nedenfor avviste også departementet flere av de andre forslagene. Fad skulle derfor heller ikke ha noen overordnet innflytelse over andre departementers oppgaver.

Neden gis en kort oversikt over viktige forskjeller mellom forslagene i NoU 1978:48 og departementets konklusjoner:

Noen av forslagene i NoU 1978: 48

- Fad skal ha det overordnede ansvar for statens databehandling
- Styrke samarbeidet mellom stat og kommune
- Vekt på å standardisere dataelementer og forenkle mulighetene for utveksling av data på tvers
- Etablere og vedlikeholde system- og utstyrskatalog
- Fastlegge felles rammer og modeller for systemutvikling, oversikt over erfaringer med bruk av ulike metoder
- Etablering av regionale drifts- og kompetansesentra og sentrale og lokale datautvalg

St. meld. 12(1982-83)

- Fad skal ha en initiativtakende rolle ,og trekke opp retningslinjer, men ikke kunne gripe inn i enkeltsaker
- Begrenset samordning eller koordinering, dette skal skje gjennom ordinære politiske og administrative organer. R-direktoratet skal ha en koordinerende rolle for standardisering
- Hensyn til sikkerhet og sårbarhet tilsier varsomhet med å etablere for omfattende fellesløsninger
- Ingen regionale drifts- eller kompetansesentra
- Opprette et rådgivende datapolitisk råd

Figur 4: Sammenheng mellom forslagene i NOU 1978:48 og St. meld. 12(1982–83)

Stortinget sluttet seg i all hovedsak til departementets framlegg. Det ble også, i tråd med meldingen, opprettet et Datapolitisk råd, som skulle overvåke IKT-utviklingen generelt.

Et resultat av meldingen var at arbeidet med datapolitikk ble styrket, og i noen grad integrert med moderniseringsarbeidet i forvaltningen generelt. Mange opplevde likevel nok derfor meldingen til Stortinget som et skritt tilbake i forhold til ønskene om en mer samordnet datapolitikk. For å sitere en av kommentarene: «*Velbegrunnet passivitet: Tilbake står vi med en melding som sier at utviklingen skal gå som den vil*» (Heitmann i Kartellnytt 15.9.82)[12].

12 Petter Hidas bringer også et sitat «Datateknikken er en av de mest verdifulle hjelpemidler som er skapt av mennesker. Det er ikke ved ensidig grubling av dens skyggesider vi får glede av den. Det får vi ved velbetenkt søken etter gode måter å utnytte de rike mulighetene som teknikken byr på.» (Polyteknisk revy 1982:8).

Vi skal her merke oss, som tidligere omtalt, at statsråd Gjertsen hadde store ambisjoner om betydelige endringer i forvaltningspolitikken, i retning mot nettopp forenkling, mindre statlig styring og privatisering og i alle fall økt konkurranse[13]. Meldingen må sies å være i tråd med dette, og derved forankret i rådende forvaltningspolitikk. I kjølvannet av dette ble Statens Datasentral omgjort til et AS i 1986 (for øvrig etter eget ønske), og R-direktoraters rolle på IKT-området ble endret til en mer rådgivende funksjon, og ikke som en aktør i markedet. Behandlingen i Stortinget sementerte for øvrig også skillet mellom statlig og kommunal databehandling, slik at vi må kunne si at forvaltningspolitikken «seiret». Samtidig bidro dette til å forsterke (eller i det minst lot vær å løse) en del problemer knyttet til kommunikasjon, samordning og forvaltning av felles datagrunnlag.

Dersom målet med politikken var å stimulere veksten i utbredelse av IKT i forvaltningen, så lyktes departementet godt. 1980-tallet preget av en nærmest eksplosjonsartet vekst innen offentlig databehandling; Norsk Datas maskiner med Tandberg-skjermer var snart å finne i alle kroker av forvaltningen; fra 15% til 90% terminaldekning i departementene fra 1982 til 1989, og det ble lagt planer for et felles bredbåndsnett i sentralforvaltningen. «La de 1000 blomster blomstre», på godt og mindre godt. Videre ser vi i denne perioden framveksten av store etatssystemer, som Trygdeetaten, Arbeidsmarkedsetaten[14], Tollvesenet (TVINN)[15] og andre. Disse ble i første omgang innført uten større organisatoriske endringer i etatene, men med innføring av FLID[16] i ligningsetaten på 90-tallet fikk vi den første store omorganiseringsprosess i en landsdekkende etat som resultat av et nytt IKT-system, hvor det også skjedde betydelige endringer, både i arbeidet ved det enkelte ligningskontor som arbeidsdelingen mellom kontorene, og hvor arbeidet ble mer spesialisert (verdiorientert ligning (Sørgaard et al. 1997)). Vi fikk også i denne perioden vår første nasjonale IT-plan (1987–90), uten at dette førte til noen spesiell satsing innen offentlig sektor (Buland 1996). Dette var kanskje typisk, at på det retoriske plan var sektorpolitikerne opptatt av IKT, mens den overordnede forvaltningspolitikken, som fortsatt ble i hovedsak styrt av Finansdepartementet, lå fast.

13 En skal kanskje være varsom med å tillegge statsrådene alle synspunkter i meldingen, da den er ført i pennen av tidligere underdirektør Svein A. Øvergaard, en kunnskapsrik og svært erfaren fagperson på feltet.

14

15 TVINN er Tollvesenets informasjonssystem med næringslivet, som gjorde det mulig for den enkelte speditør å fylle ut skjema ved import av varer. Det første systemet som tillot brukerne å delta aktivt i saksbehandlingen?

16 FLID: Folkeregister og Ligningskontor; Innføring av Data. Se f eks. Harket (1996)

Men denne veksten skapte også problemer, både gamle og nye, gjennom et villnis av ulike løsninger som ikke enkelt kunne kommunisere og utveksle data. Vi fikk derfor på slutten av 80-tallet to nye og viktige utredninger: Først kom NOU 1988:15 *Samspill om Grunndata* som bidro til at arbeidet med et nytt Enhetsregister og senere Oppgaveregistret kom i gang. Gjennom NOU 1988:40 Datapolitikk i staten ble igjen mange spørsmål knyttet til fellessystemer generelt og problemene knyttet til manglende kommunikasjon og samhandling satt på dagsorden. Oppfølgingen av utredningen bidro til at R-direktoratets arbeid med fellessystemer ble avsluttet og overført til Statens datasentral, og ansvaret for regelverk sammen med kravspesifikasjonene ble lagt til de respektive forvaltningsorganer. Dette var en understrekning av at de generelle prinsippene om ansvar for egen oppgaveløsning også gjaldt ved bruk av IKT-systemer.

En annen viktig begivenhet var igangsetting av prosjektet *Nasjonal infrastruktur for edb* (1988–1992) i regi av Statskonsult, hvor en forsøkte å etablere et forpliktende samarbeid mellom de store statlige etatene[17]. En rekke prosjekter ble gjennomført, og sjøl om det ikke resulterte i konkrete løsninger som ble satt i drift, var nok erfaringene fra disse prosjektene verdifulle for senere arbeid. Men spesielt må nevnes at Kgl. res av 6.12.1991 hvor Arbeids- og administrasjonsdepartementet får hjemmel til å pålegge statsforvaltningen å bruke standardprodukter og hvor spesielt NOSIP[18] ble definert som standard for datakommunikasjon. Ettertiden har imidlertid vist at dette pålegget var uklokt, og i dag har Internett-standardene overtatt.

I St. meld 35(1991–92) ble disse innsatsområdene knyttet til IKT framhevet: i) Offentlig informasjon som felles ressurs ii) datakommunikasjon og informasjonsutveksling iii) IT-standardisering og iv) utvikling av konkrete IKT-systemer. Videre ble det fremmet en sektorplan for IT i forvaltningen 1993–1996, hvor Aad for alvor påtar seg rollen som initiativtakende og pådrivende aktør for IKT i forvaltningen. Dette illustrerer derved at IKT nå blir en mer sjølstendig del av forvaltningspolitikken, uten at IKT-politikken nødvendigvis går på tvers av denne. Det ble i denne perioden også utformet andre sektorplaner for IKT, blant innen helse- og skolesektoren.

Etter Internett fikk sitt endelig gjennombrud i 1994/95 ser vi at IKT forventes å spille en mer framtredende rolle som pådriver. Dette er svært tydelig

17 Disse var med: Skatte-, Trygde-, Arbeids, og Tolletaten, Statistisk sentralbyrå, Televerket og Postverket

18 NOSIP (Norsk OSI-profil) er en forvaltningsstandard for datakommunikasjon, basert på de internasjonale standarder, blant annet X.400. Disse var omstridt, fordi de ikke samsvarte med Internett-protokollene som for alvor var på vei inn i så vel forvaltningen som samfunnet generelt.

i rapporten fra Statssekretærutvalget for IT «Den norske IT-veien Bit-for-Bit» fra 1996 (Sd 1996). I rapporten, som har en tydelig et teknologioptimistisk (endog teknologideterministisk) tone, framhever Regjeringen, nærmest i panegyriske vendinger, hvilken rolle teknologien skal spille i utviklingen av så vel forvaltningen som samfunnet generelt. Uten å ta meldingen for bokstavelig, kan vi slå fast at IKT nå oppfattes som en samfunnsomdannende faktor, hvor verktøyperspektivet bare er en av flere dimensjoner. De senere planer, jf eNorge 2005, eNorge 2009 og endelig St.meld. 17(2006–2007), endrer ikke dette bildet, sjøl om tonen er noe mer nøktern. I dag er imidlertid alle spørsmål knyttet til IKT-utviklingen generelt i samfunnet lagt til Fad. Det som imidlertid står fast er at de grunnleggende ansvars- og myndighetsforhold ikke er endret, og at Fad ikke er noe overordnet IKT-departement.

Samordning og felles forvaltning av datagrunnlaget

Et sentralt og tilbakevendende tema har vært samordning og enhetlig forvaltning av felles data (også kalt grunndata), og blant annet diskusjoner omkring sentrale eller lokale folkeregistre. Allerede i 1970 kom et forslag om at personregistret under folketrygden bør bli et felles nasjonalt register (LPD 1970). Samordning og kvalitetssikring av data var sentralt i Elgsaasutvalgets rapport, og ble drøftet både i NOU 1988:15 og NOU 1988:40. I forberedelsene til etablering av KOSTRA ble problemene rundt kvaliteten på ulike registre drøftet, med forslag om å sentralisere forvaltningen av sentrale databaser (Jansen 1993) [19]. Forslagene ble stort sett avvist. Samtidig har det skjedd en betydelig samordning, ikke minst gjennom etablering av Oppgaveregistret i 1997[20] og både når det gjelder innrapportering (gjennom AltInn) og forvaltning av slike data i BRREG. Sentral eller lokal dataforvaltning berører en rekke spørsmål, også av prinsipiell karakter:

i. *Den politiske styringen og ansvar og myndighet*. Alle opplysninger som danner grunnlag for beslutninger i forvaltningen er hjemlet og definert i lov og forskrift, og derved uttrykk for en politisk beslutning. Disse kan derfor ikke uten videre samordnes uten at det gjøres eksplisitte endringer i det rettslige grunnlaget. Den rettslige forankringen bestemmer også hvilket

19 Senest i 2004 ble det i den såkalte daVinci-rapporten foreslått å samle alle personopplysninger i et felles register.

20 NHD har i brev av 18.06.2002 pålagt statlige virksomheter å sørge for at alle data i tilknytning til elektronisk innrapportering fra næringslivet til det offentlige skal bygge på Oppgaveregisterets database.

forvaltningsorgan som har myndighet til å innhente og forvalte dataene (Schartum og Jansen 2004).

ii. *Kvalitet og kontroll*. Erfaringer synes å vise at god dataforvaltning skjer best nært kilden eller der kompetansen for å vurdere kvaliteten av dataene sitter. Sentral forvaltning av data som skapes eller endres lokalt skaper ofte problemer.

iii. *Tilgjengelighet og bruk*. Lokal forvaltning (f.eks. i kommunene) kan skape problemer vedr. tilgjengelighet, og ikke minst rasjonell gjenbruk dersom dette ikke er organisert gjennom forpliktende samarbeid og basert på et nødvendig sett av felles standarder.

iv. *Personvern, sikkerhet- og sårbarhets*hensyn, som reiser viktige utfordringer både ved sentral og lokal dataforvaltning.

Generelle forvaltningspolitiske prinsipper tilsier institusjonssvis (lokal) forvaltning der dette er knyttet til det enkelte forvaltningsorgans oppgaveløsning. Argumenter som f.eks. tilgjengelighet og effektivitet kan tale for sentral forvaltning. Altinn og Brønnøysundregistrene sammen SSB's registre representerer en sentral modell, mens vi ellers har betydelig grad av lokal dataforvaltning. Etableringen av BRREG og utviklingen av Altinn er basert på de mulighetene som er skapt av teknologien. Løsningene gir både gode brukertjenester og store effektiviseringsgevinster, men samtidig har en ennå ikke løst alle spørsmål knyttet til ansvar og myndighet (Naomi 2006).

4. Andre politikkområder av betydning for forvaltningspolitikken

IKT-politikken har vært influert av andre politikkområder, ved at denne teknologien er blitt sett på som et viktig virkemiddel for andre mål. Her vil vi kort se på noen nærings- og distriktspolitiske sider.

Næringspolitikkens innflytelse på IKT-politikken

Industri- og senere næringspolitikken har vært opptatt av målrettet forskning og utvikling, gjennom et nært samarbeid mellom staten og næringslivet. Datateknologien har her vært sentral, gjennom at forskningen skulle kunne kommersialiseres i norskbaserte databedrifter. Eksempler er SIMULA, Nord Data maskiner, Tandberg-skjermer, den tidlige utviklingen av telenett-teknologiene med mer (Haraldsen 2005).

Hensynet til norske industriinteresser har også vært en viktig faktor i forvaltningens IKT-politikk, med eksempler som samarbeidet mellom Norsk data og R-direktoratet (SISU-prosjektet med mer) og ikke minst deling av trygde-Norge

i Infotrygd og NorTrygd[21]. Den dominerende stilling som Norsk Datas produkter hadde i statlig og kommunal forvaltning kan i ikke ubetydelig grad tilskrives tette bånd mellom bedriften og sentrale personer i forvaltningen og på politisk nivå. Argumentene var særlig to: i) Det var etter hvert et uttalt mål at forvaltningen skulle utgjøre et krevende marked for næringslivet, og derved gjøre norske produkter konkurransedyktige i utlandet. ii) En moderne forvaltning med ansatte som behersket ny teknologi ble sett på i seg sjøl som en konkurransefaktor. Dette ble allerede hevdet i den første nasjonale IT-planen fra 1987, og er blitt gjentatt i de fleste senere IKT-dokumenter. Argumentet står vel enda sterkere i dag, da det framheves både nasjonalt og internasjonalt hvor viktig det er for landene å være langt framme i spredning og bruk av IKTE (f.eks. målinger av e-readiness, og de enkelte lands innsatser når det gjelder å tilby offentlig tjenester helelektroniske). Det synes i dag helt klart at teknologiutviklingen i stor grad influerer på politikken, både i forvaltningen og generelt det politiske landskapet.

Likeledes ser vi at på det distriktspolitiske område er IKT blitt brukt som et viktig virkemiddel, og IKT har bidratt til et ikke ubetydelig antall arbeidsplasser i grisgrendte strøk, med eksempler som Brønnøysund, Mo i Rana, Kirkenes, Leikanger, Vardø osv. Likevel er det grunn til å reise spørsmål om den retoriske kraften i distriktspolitikken har vært sterkere enn de faktiske effekter, da ulike studier viser at IKT-utviklingen i minst like stor grad har bidratt til sentralisering (Jansen 1998).

5. Diskusjon og foreløpige konklusjoner

Den forutgående, noe fragmenterte gjennomgangen av IKT-utviklingen i forvaltningen viser et mangeartet bilde, men det etterlater seg likevel et inntrykk av at de grunnleggende trekk ved den norske forvaltningen ligger fast, og de endringer som har skjedd norsk forvaltning, har vært resultat av politiske beslutninger hvor teknologien stort sett er blitt brukt til å nå generelle politiske mål. Med basis i den skjematiske tabellen presentert innledningsvis kan vi sammenstille noen av resultatene på denne måten:

21 Saksbehandlersystemene Infotrygd ble utviklet av Kommunedatasentralen Øst (på Hamar) i samarbeid med RTV/Oslo trygdekontor basert på IBM-plattform, mens NordTrygd ble utviklet av Norsk Data i samarbeid med R-direktoratet. Oslo og de store byene fikk Infotrygd, de mindre kommunene fikk Nortrygd. Systemene ble innført i perioden 1984-1986.

	Forvaltningspolitikken		IKT-politikken		
	Visjon og mål	Virkemidler	IKT-forståelse	Mål for IKT-bruken	Typiske Virkemidler
1955 – 1970	Vekst i velferdsstaten	Kostnads-effektivitet og rasjonalisering	Verktøy for automatisering	Rasjonalisering ved automatisering av rutineoppgaver	Stormaskiner og datasentraler
1970 – 1985	Videreutvikle velferdsstaten	Delegering og desentralisering	Desentralisering og distribusjon	Støtte for saksbehandling og andre kontorfunksjoner	Minimaskiner og individuelt kontorstøtteverktøy
1985 – 1995	Brukerorienteri ng og fornyelse	Målstyring, fristilling og økt konkurranse	Nettverk og infrastruktur for samhandling	Integrasjon av IKT i alle arbeidsprosesser nye samarbeids-mønstre	Standardisering, etablering av felles datagrunnlag
1995 – 2005	Sikre rettigheter og økt valgfrihet	Økt tilgjengelighet og tjenestekvalitet	Informasjons-samfunnet og Cyberspace	Elektroniske tjenesteyting over Internett	Endrer samhandling forvaltningen og innbyggerne. Transformasjon av organisasjoner.

Tabell 3: Mål i forvaltningspolitikken sammenholdt med mål for IKT-bruken

Denne skjematiske oversikten indikerer at det ikke har vært grunnleggende motstrid mellom den generelle forvaltningspolitikken og de mål og virkemidler som har vært definert for IKT-bruken. Nå er det ikke overraskende at den parlamentariske styringskjeden i hovedsak har fungert, og fagdepartementer og det enkelte forvaltningsorgan forholder seg til fastlagte myndighetsforhold. En ser imidlertid en utvikling hvor teknologien får en stadig viktigere rolle, noe som er ønskelig fra mange hold, både fra næringslivet og politikerne.

Nå innebærer imidlertid ikke dette at all innføring av IKT har fulgt en gjennomtenkt plan, og heller ikke at en har oppnådd de ønskede resultater. Det er nok av eksempler på ambisiøse planer og feilslåtte prosjekter, slik vi også finner for øvrig i samfunnet. Samtidig er det mange som mener at IKT-utviklingen i forvaltningen ikke går fort nok. Vi har de siste 10 år sett et betydelig press i retning av at bruk av IKT er blitt ett mål i seg sjøl, f.eks. ved å få flere offentlige tjenester elektronisk tilgjengelig for at flest mulig av borgerne skal bruke disse elektroniske tjenestene. Vi også sett i de senere år at politikerne har igangsatt «flaggskip-prosjekter», gjerne for å vise handlekraft eller at de «følger med « i teknologiutviklingen, men som ikke er forankret godt nok i organisasjonen.

Har IKT-utviklingen bidratt til å endre maktforholdene mellom departementene? Som vi har sett, var det Finansdepartementets ansvar, dog motvillig, å akseptere initiativet fra ligningssjefene på Vestlandet på 50-tallet. Nesten samtidig begrunner departementet anskaffelse av den første datamaskin i staten, som illustrerer både toppstyrte og «grasrot-initiativer». Begrunnelsene for begge forslag var rasjonalisering og effektivisering. Opprettelsen av Fad i 1972 gav dette departementet en overordnet rolle i utviklingen av statsadministrasjonen, og etter hvert også ansvar for statens IKT-politikk. Men Fad er

aldri blitt noe superdepartement for IKT-spørsmål (noe mange i næringslivet ønsker), og det er utvilsomt Finansdepartementet som fortsatt holder «hånden på rattet» når det gjelder beslutninger utover det enkeltes forvaltningsorgan eller fagdepartements myndighet.

Bør det være slik? Nå kan ikke forvaltningspolitikken være et mål i seg sjøl, dersom det hindrer forvaltningen i å oppnå andre prioriterte mål. Mye av kritikken mot dagens IKT-løsninger i forvaltningen er at tjenestene ikke er godt nok utviklet på tvers av forvaltningsorganer og sektorer. Fortsatt råder «silo-tenkningen», som viser at samordning er krevende, både på beslutningsnivå, men også når det gjelder organisering. Dette er blant annet påpekt i en OECD-rapport som har vurdert den norske IKT-satsingen (OECD 2005).

Bør vi da heller stille spørsmålet slik: Har rådende forvaltningspolitikk hindret en rasjonell utnyttelse av IKT og utvikling av gode brukertjenester? Burde myndighetene lyttet mer til de mange anbefalinger og etter hvert tydelige krav om sterkere grad av samordning? Skaper den sterke vektlegging av desentralisering og delegering unødvendig store barrierer mot å realisere gode fellesløsninger? Resultatene av denne studien gir så langt ikke noe entydig svar, men det kan pekes på et par sentrale utfordringer.

i. Kan store, byråkratiske organisasjoner makte å være tilstrekkelige innovative? Det synes å være en rådende oppfatning at nytenkning og omstilling skjer oftere og lettere i mindre og mer dynamiske organisasjoner. Vi har imidlertid sett gode eksempler på innovasjoner internt i den enkelte forvaltningsorgan, men det er langt mer krevende når det involverer flere virksomheter og krever beslutninger.
ii. Er dagens forvaltningsstruktur egnet til å håndtere de nye informasjonsinfrastrukturer som vokser fram? Mens de tradisjonelle IKT-løsningene i forvaltningen utgjør relativt statiske og kontrollerbare informasjonssystemer, ser vi nå at de nye løsningene, som Enhets- og Oppgaveregistrene, Altinn, Samordna opptak, KOSTRA etc. skal fungere som underliggende infrastrukturer som mange andre systemer og anvendelser er avhengig av. Dette innebærer nye krav til så vel tilgjengelighet og stabilitet som fleksibilitet og dynamikk (jf f eks Monteiro 2000). Slike infrastrukturer formes gjennom et samspill av tilbydere og brukere, og kan ikke kontrolleres på samme måte som tidligere og skaper nye avhengighetsforhold (Star and Ruhleder 1996, Ciborra 2000).
iii. Store IKT-prosjekter, både i forvaltningen og ellers, innebærer betydelig risiko. Det har vi sett tydelig illustrert i de omfattende infrastrukturprosjektene i blant annet Statoil og Hydro. Hvordan er forvaltningen rustet til å håndtere usikkerheten og risikoen i tilsvarende tverrsektorielle prosjekter,

er f. eks. dagens tradisjonelle styringsstruktur velegnet for dette? Det er derfor viktig å studere hvordan *risiko* faktisk kan og bør håndteres i en virkelighet med økende kompleksitet og avhengighet (Sørgaard 2006). Det gjelder å studere premissene for valg av teknologi og hvilke normative evalueringsstandarder som er rådende.

Sluttkommentaren blir da: Hva kan vi lære av historien når vi skal møte morgendagens utfordringer? Det bør være relevant å ha kunnskaper om de erfaringer som er gjort med forvaltningspolitikken generelt og IKT-politikken spesielt. Vi må kjenne hvilke barrierer som eksisterer og hvorfor det så vanskelig å fjerne disse, for å få til de ønskede endringene.

Referanser

Aberbach, Joel D. and Tom Christensen (2005): *The challenges of modernizing tab administration: Putting customers first in coercive public organizations. Paper presented at the annual meeting of the American Political Science Association, Marriott Wardman Park, Washington, DC*, Sep

Andersen, J. A. og B. Abrahamson (1996) Organisasjon. Om å beskrive og forstå organisasjoner. Cappelen Akademiske Forlag, Oslo.

Boe, Erik (1993): *Innføring i juss bind* 2 Tano, Oslo,

Buland, Trond *Den store planen. Norges satsing på informasjonsteknologi 1987–1990* Rapport 27/96 Senter for teknologi og samfunn, NTNU, Trondheim

Christensen , Tom og Morten Egeberg (1997) *Forvaltningskunnskap*. TANO, Oslo

Christensen, Tom og Lægreid, Per (2001) New Public Management , Ashgate Publ. Company.

Christensen , Tom (2002) *Forvaltning og politikk*. Universitetsforlaget. Oslo

Christensen, Tom, Per Lægreid, Paul G. Roness (2004) *Organisasjonsteori* for offentlig sektor. Universitetsforlaget, Oslo

Ciborra, Claudio (2000) A Critical review of the literature on the Management of Corporate Information Infrastructures In Ciborra et al: *From control to drift*. Oxford University Press.

Colbjørnsen, Tom (2004) *Modernisering og fornyelse i staten*. Rapport til Moderniserings-departementet, Oslo

Eriksen, Svein (2001) *Departementstrukturer I Norge, Storbrittania, Sverie, Finland og Danmark*. **Rapport Statskonsult,**

Fad (1986) *Program for modernisering av statlig forvaltning*, Forburker- og ad. departementet, 1986

Fimreite, Anne Lise (2006) KOSTRA – et hinder for eller et verktøy i lokaldemokratiet. I Tranvik (red.) *Digital teknologi og organisasjonsendring*. Fagbokforlaget, 2007

Hanseth, Ole, Claudio Ciborra og Kristin Braa (2001) The Control Revolution. The EPR and the side effects of globalisation . *The Data Base for advances in Information Systems* 32(4) 34–46

Haraldsen, Arild (2003) *50 år og bare begynnelsen*, Cappelen. **Oslo**

Harket, Even 1996) *Oppgaveplikt og ligning i omstillingens tegn. Hovedfagsoppgave ved Avd. for forvaltningsinformatikk*, UiO, URL: http://www.afin.uio.no/forskning/hovedfag/harket.pdf. Lest

Inst. Nr. 72 fr administrasjonskomiteen om Statens rasjonaliseringsdirektorats virksomhet i 1973.

Inst. S. nr 171 (1982–1983) *Innstilling fra forbruker og adm. komiteen om Desentralisering og effektivisering i den offentlige databehandling og spørsmål om datapolitiske organer.*

Jansen, Arild (1993) *Datautveksling mellom Kommune og Stat*. Rapport 1993:15. Statskonsult

Jansen, Arild: *Utkanten i den globale Landsbyen. Integrasjon eller Identitet*. Dr. Scient. avhandling 15:1998. Inst. For Informatikk, Universitetet i Oslo, ISBN: 82–7368–199–8

Lintvedt, Mona Naomi (2006) Altinn – en systembeskrivelse. I Schartum (red) *Elektronisk forvaltning i Norden Fagbokforlaget*. ISBN 978–82–450–0554–7.

LPD (1970) *Innstilling om Felles datasentral for administrative oppgaver i staten* Avgitt av komité 25.juni 1970

Lægreid, P.& Christensen,T.(1998): *Den moderne forvaltning. Om reformer i sentralforvaltningen*. Oslo Tano Aschehoug.

Nylehn, Børre (1997) *Organisasjonsteori*. Kolle Forlag ISBN 82–462–0007–5

NoU 1973: 43 *Om Planlegging av databehandlingen.*

NOU 1978:48 Offentlig databehandling Desentralisering og effektivisering

NoU 1988: 15 *Samspill om Grunndata*

NoU 1988: 40 *Datapolitikk i Staten*

NoU 1989: 5 *En bedre organisert stat*

Se OECD (2005) ICT diffusion to business: peer review country report: Norway URL: http://www.regjeringen.no/upload/kilde/aad/red/2004/0118/ddd/word/220353–040914_endelig_oecd-rapport_it-politiske_utfordringer.doc

Schartum, Dag Wiese og Arild Jansen (2004) *Høring – Forprosjektrapport om arkitektur for elektronisk samhandling i offentlig sektor.* http://www.afin.uio.no/forskning/notater/AFIN

Sd (1996) *Den norske IT-veien – Bit for Bit*. Rapport fra Statssekretærutvalget for IT til Samferdselsdepartementet

Star, S.L. and K. Ruhleder (1994) Steps to an ecology of infrastructure *Information Systems Research* 7/1 111–134

St.mld. 37 (1974–1975) *Om Planlegging av databehandlingen.* Forbruker- og adm.departemenet

St.mld. 31 (1975–1976) *Administrativt utviklings- og effektiviseringsarbeid.* Fad

St.mld.12 (1982–1983) *Desentralisering og effektivisering i den offentlige databehandling og spørsmål om datapolitiske organer* Forbruker- og adm.departemenet

St.meld. nr. 35(1991–92) Om statens forvaltnings- og personalpolitikk. Arbeids og adm.dep.1992

St. mld. 17 (2006–2007) *Eit Informasjonssamfunn for alle*. Fornyings- og adm. dep, 2006

St. prp. 85 (1971–1972) *Om endringer i bevilgninger på statsbudsjettet for 1972 under kap. 22*

Statskonsult (2006) *Utviklingstrekk i forvaltningspolitikken fra ca 1990.* Rapport 10: 2006

Sørgaard, Pål (2004) Co-ordination of E-government .Chapter 4, pp 53–77,in Jan Damsgaard and Helle Zinner Henriksen (eds), *Networked Information Technologies: Diffusion and Adoption*.Kluwer Academic Publishers, ordrecht, 2004. ISBN 1–4020–7815–3

Sørgaard, P, I. Solheim, A. Kluge Riita Hellman (1997): *IT i offenlig sektor,* Universitetsforlaget.

IDENTITY MANAGEMENT AND DATA PROTECTION LAW

RISK, RESPONSIBILITY AND COMPLIANCE IN 'CIRCLES OF TRUST'

Thomas Olsen and Tobias Mahler
Norwegian Research Center for Computers and Law (NRCCL)
University of Oslo, Norway

Abstract:

Today, we are expected to remember a different user name and password for almost every organisation or domain we want to access on the Internet. Identity management seeks to solve this problem by making digital identities transferable across organisational boundaries. The basic idea is that the participating organisations will set up a collaboration (or ***circle of trust***) which involves both ***identity providers*** and other service providers. However, there is a risk that identity management may reduce the users' level of privacy: Can the collaborating organisations collect personal information and create a profile which includes the user's interaction with all collaborators? Who is responsible for the processing of personal data if many organisations collaborate? How can the user make informed decisions and consent to the processing of his data? This article seeks to address these issues from the perspective of European data protection law.*

---

* This article was previously published in *Computer Law and Security Report*, vol. 23(4) 2007, pp. 342-351 and vol. 23(5) 2007 pp. 415-426. The research presented in the paper was partly funded by the European Commission through the IST programme under Framework 6 grant to the Legal-IST project and partly financed under the Research Council of Norway through the projects ENFORCE and PerProt. The authors would like to thank Clive Seddon, Vicky Cooper, Sarah Williams at Pinsent Masons (UK) and Miguel Valdes and Sergio Morales Valdes at Garrigues (Spain) for their contribution to the Legal-IST report D11 'Privacy – Identity Management', 4 November 2005 (available at www.legal-ist.org). This paper expands on our contributions to the report, acknowledging the valuable input received from the report's co-authors. We also thank Professor Dag Wiese Schartum, Professor Jon Bing, Line Coll, Herbjørn Andresen and Rebecca Wong for valuable comments to earlier versions of this paper.

1 Introduction

The extensive use of organisation-specific user names and passwords is often considered cumbersome by consumers who rapidly want to access an IT resource.[1] The desire to find more user-friendly and efficient ways of managing digital identities, has led to the development of identity management systems which allow the passing of electronic identities across organisational boundaries. This collaborative use of electronic identities within and across multiple organisations' information systems (*multi-organisation identity management*) raises technological as well as organisational and legal questions.[2] In terms of technology, collaborators need to decide upon an architecture that supports the communication of identification data. On the organisational level, collaborators need to integrate some of their business processes in order to achieve interoperability. From a legal point of view, cooperation about identity management is challenging in terms of the necessary contractual framework, the allocation of liability and, last not least, the protection of personal information. This paper focuses primarily on the latter issue, i.e. on privacy and data protection law related to electronic identities in a multi-organisational setting.

The technologies that currently are under development and the way these are to be implemented will probably have a major impact on the way we communicate and collaborate through the Internet in the future.[3] Identity

1 In the Norwegian press this topic has sometimes been discussed under the title 'tyranny of passwords', see e.g. Mona Sverrebo Halland, Passordtyranniet, Dagens Næringsliv, 14 September 2004.

2 See, e.g. Hansen, M. and Meints, M., 'Digitale Identitäten – Überblick und aktuelle Trends. Identity-Lifecycle, Authentisierung und Identitätsmanagement', Datenschutz und Datensicherheit 30 (2006), pp. 543-547 and Dumortier, J. and Goemans, C. ‚Legal Challenges for Privacy Protection and Identity Management', in: Proceedings of the NATO/NASTEC Workshop on Advanced Security Technologies in Networking, Bled (Slovenia) 15-18 September 2003, Springer, 2004, p. 191-212. http://law.kuleuven.ac.be/icri/publications/610Dumortier_Bled_Paper.pdf?where=, last visited 8 March 2007.

3 Microsoft's recent initiative for an identity metasystem is arguably of particular importance. See, e.g. Microsoft, 'The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity', www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf, last visited 08 January 2007. The identity metasystem is an overarching framework that enables identity systems to interoperate with one another. It builds on the premise that one single, universal identity management system for the Internet would be misguided and counterproductive with respect to security and privacy. The metasystem is based upon an underlying set of principles, 'The seven Laws of Identity', developed through an open consensus process on the Internet. The laws are intended to codify a set of fundamental design principles to which a universally adopted, sustainable identity architecture must conform. Interestingly, the design principles have parallels with general principles found in most international data protection instruments, including the EU Data Protection Directive, see e.g. Cavoukian, A., '7 laws of identity – the case for privacy-embedded laws of identity in

management systems are an important research focus for many European research projects and international collaborations, and some of these projects have an explicit focus on privacy-enhancing functionalities.[4] It is important that researchers and those implementing the technologies are aware of the legal issues and able to design multi-organisation identity management systems in compliance with the European legal framework for data protection law.

This paper explores how a network of organisations can manage the responsibility for compliance with European data protection law.[5] European data protection law does not provide specific rules for identity management. Instead, it more generally addresses the processing of personal data by one or more organisations (controllers and processors), and it provides conditions for the lawfulness of such processing. Our analysis of data protection issues in multi-organisation identity management will be at three levels, covering 1) the use of information technology, 2) organisational issues of collaboration and 3) the interaction with the end-user, as illustrated in Figure 1.

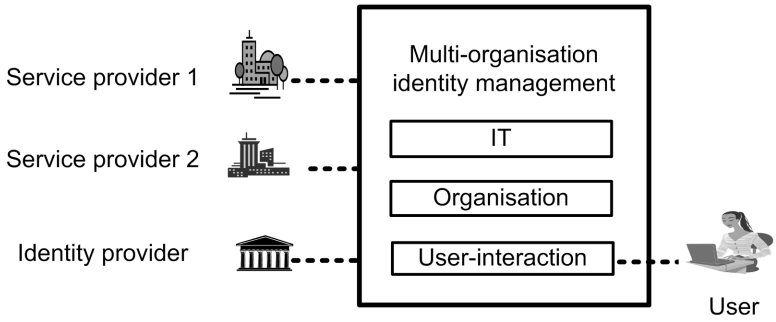


Figure 1 – Identity management involving multiple organisations

the digital age', Information and Privacy Commissioner of Ontario, 2006. Microsoft's Windows CardSpace (formerly 'InfoCard'), which at times of writing has not yet been launched, is an example of an identity selector that conforms to the seven laws of identity, see Chappell, D. 'Introducing Windows Cardspace', April 2006. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnlong/html/IntroInfoCard.asp, last visited 08 January 2007.

4 See e.g. PRIME (Privacy and Identity Management for Europe), https://www.prime-project.eu/; FIDIS (Future of Identity in the Information Society), http://www.fidis.net/; and GUIDE (Government User IDentity for Europe), http://istrg.som.surrey.ac.uk/projects/guide/. For an overview of current projects (in German), see Meints, M. and Hansen, M., 'Identität – die europäische Perspektive', Datenschutz und Datensicherheit 30 (2006) pp. 531-532.

5 European data protection law consists of a number of directives, notably the Data Protection Directive 95/46/EC, the Directive on Privacy and Electronic Communications 2002/58/EC and the Directive on Data Retention 2006/24/EC. See further Section 3.1.

Firstly, identity management involves a number of IT issues which have an impact on privacy and data protection. For example, the design of identity management systems and the utilization of identifiers may affect users' control over personal data. Secondly, data protection law will have an impact on how the collaboration is administrated at an organisational level. The responsibility for certain business processes may imply legal liabilities and responsibility for compliance. Thirdly, the interaction with the end-user is essential from a data protection perspective and will have an impact on how the end-user perceives the service. Users' trust in the system may be partly based on the user-interface, and this interface needs to include legal notices informing the users about how their data will be processed.

These three layers of IT, organisation and user interaction are to some degree reflected in the structure of this paper. Initially, section 2 describes and analyses existing and emerging solutions for identity management, in particular Microsoft .NET passport and Liberty Alliance. In order to understand the data protection issues, it is to a certain extent necessary to review *IT* details such as the handling of identifiers. Subsequently, section 3 addresses the *organisational* aspects of identity management, analyzing how the responsibility for compliance with data protection law can be administered. The law offers a limited set of legal roles (controller, processor), which need to be mapped to the organisational roles in identity management. The perspective shifts in section 4, where we examine the *communication between the end user and the collaborators*. This interaction needs to be compliant with inter alia the obligations to inform the user about how personal information will be utilized, which may be challenging in a multi-organisational setting. We therefore explore mechanisms to provide user-friendly simplified information and we analyze the possibility of employing specific technical mechanisms which may increase transparency and give the end-user means to control the disclosure of personal data. Finally, section 5 draws the conclusions of this analysis both with a view to give suggestions to how multi-organisation identity management should be set up and *de lege ferenda* as policy issues to be considered by the European legislators.

2 Identity management

Identity management is, in itself, not a new concept, even though the term seems to be of recent origin.[6] Governments and private entities have for a long time issued ID cards or other documents to individuals for identity authentication

6 See e.g. Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, p. 1.

or as a proof of privileges in future interaction.[7] However, the phrase identity management has usually not been used for the administration of these traditional documents, even though there are similarities between paper-based and IT-based identity management schemes. Identity management does not refer to a single specific system, but rather to a category of interrelated solutions, utilized to administer user authentication, access rights and restrictions, account profiles, passwords, and other attributes.

In the following sub-sections we will first describe some key aspects of identity management. We will then review the spectrum of identity management approaches and introduce two examples (respectively Microsoft .Net Passport and Liberty Alliance), which will be analysed in the remainder of the paper. The analysis of these examples will focus on identifying risks to privacy.

2.1 Key aspects

Identity management systems can be used to support a controlled access to resources which for some reason are being restricted to certain users. The current practice is to require the user to open an account and then login to this account by means of an identifier and one or more authenticators (e.g. a username and a password). Following the terminology suggested by Clarke[8], this procedure can be divided into three general phases: 1) *pre-registration* or enrolment, i.e. registration of the user and issuing one or more identifier(s) for that user and providing the user with authenticators for later access, 2) *authentication*, i.e. the presentation of an identifier and the use of authenticators to verify the legitimate use thereof, and 3) *authorisation*, i.e. once authenticated – what privileges does this user have with regard to the services? The focus of identity management is on how to rationalise the three processes mentioned above.

Notably, *identification* is not included in this enumeration. This concept is ambiguous and will thus not be used in this paper. We need to distinguish two

7 The purpose of these physical documents is primarily to authenticate the carrier and to serve as proof of certain privileges, e.g. the right to drive a car or to the disposal of a bank account. While we are familiar with these traditional ID documents for physical identification, they are of little help for identification and authentication in the digital world. Such physical documents must meet two basic requirements to be appropriate as ID; they must contain one or more authenticators that make it possible to authenticate the card holder (e.g. signature or photograph) and the document itself must be tamper proof so that one can have a sufficient degree of confidence that the document is authentic and issued under the right procedures. See, e.g. Bing, J. and Fog, J., 'Fem essays om ny informasjonsteknologi, forbrukere og personvern', Nordisk Ministerråd, 1989, pp. 64-73.

8 Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, p. 3.

situations, which both could be called identification: Firstly, identification could refer to the process of obtaining an identifier for a user. This identifier will be used to distinguish this user from other users.[9] Secondly, the term could be used for the process of identifying the individual behind an identifier.[10]

The core function of multi-organisation identity management systems is to delegate the authentication of users to an identity provider with the aim of providing those users access to an organisation's resources. This implies that the service providers need to trust the identity provider with respect to the authentication of users. This requires diligence not only with respect to the authentication itself, but also with respect to all prior phases. Hence, one of the most evident issues to address is the strength and quality of pre-registration and authentication procedures made by identity providers. According to Roger Clarke,[11] this is an aspect that is often poorly understood and underestimated: 'The scheme descriptions are generally silent about the registration phase as a whole, and about the pre-authentication processes that are to be undertaken'.

'*Single sign-on*' is a central feature of many identity management systems. It provides users with a more seamless user-experience when accessing different user accounts on the Internet. It enables a user to access multiple sets of resources after being authenticated just once (Fig 2).[12][13]

9 In practice, many internet services do not need to know the identity of the person behind a user name. It suffices to to verify that the user is the same as the user who earlier enrolled in the service.

10 The latter understanding seems to be the basis for the definition of personal data in Article 2 of the Data Protection Directive, see below section 3.1.

11 Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, p. 36.

12 A distinction needs to be made between authentication (the process whereby confidence is established in an assertion of identity) and authorisation (what rights does the user have). Authentication of the user is most often carried out by an identity provider, i.e. a third party. The authorisation to resources and applications provided by a service-provider is most often managed by the service-provider.

13 Figure 2 is quoted from Pfitzmann, B., 'Privacy in Enterprise Identity Federation: Policies for Liberty Single Signon' Proc. Workshop on Privacy Enhancing Technologies, Springer Verlag, 2003. She describes the single sign-on process as follows, 'When the user wants to log in (or to send attributes in more general protocols), the service provider redirects the browser to the user's identity provider. The user logs in there, typically with a fixed user ID and password. The browser and identity provider may also reuse a secure session from another recent login. The identity provider then redirects the browser back to the service provider with some ticket. If the information to be transferred is short, it can be completely included in this ticket. Most protocols also provide a back channel for transferring longer information; the ticket then contains a handle to that information so that the service provider can associate a returning browser with the appropriate back-channel information.'

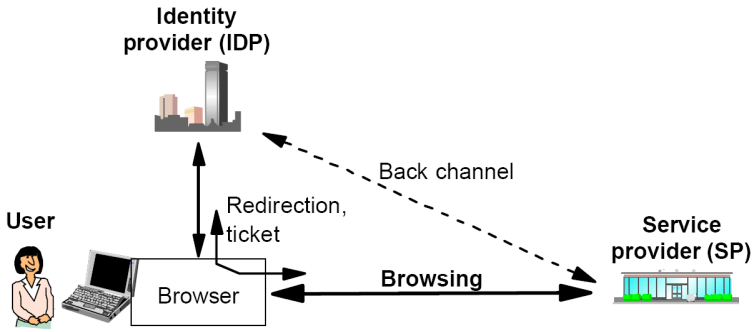


Figure 2 – Single sign-on

2.2 The spectrum

Identity management is still an emerging area, and new developments are driven by actors with different interests in mind.

At one end of the spectrum[14] we find the business-driven schemes which sometimes neglect the interests of individual users. In the early phases of the Internet, most organisations carried out identity management themselves. However, with standardisation and outsourcing came the opportunity to have some of these processes performed by third parties. Many organisations have seen the opportunity to rationalise their business processes by having common procedures and infrastructures. At the same time, identity management is seen as a convenient way to simplify the access to IT resources for employees and customers. The potential benefit of these schemes is that it may be cost-effective for organisations to outsource the authentication to one specialised identity provider. Also, such schemes provide for the possibility of sharing or passing on the current customers to collaborating business partners. Single sign-on based on Microsoft .NET Passport arguably represented

14 Even information systems with the aim of profiling user's behaviour and preferences as part of e.g. personalised services or CRM have sometimes been seen as identity management systems. A characteristic of these is that the user's profile or 'identity' is derived or abstracted from observing the user's behaviour and use of the system. See FIDIS 'Structured Overview on Prototypes and Concepts of Identity Management Systems', D3.1, September 2005. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

the most business-oriented solution for managing customers' access to multiple websites and resources after a single authentication procedure.

At the other end of the spectrum we find user-centric identity management, which seeks to raise the degree of control the user has over his digital identities and to enable the user to decide autonomously about the disclosure of his personal data.[15] Here, the focus is on the user's management of his own identities and on using the right identity in the right context. As citizens and customers with multiple relations, we have many partial identities[16] (normally referred to as 'user accounts'), e.g. in our relationships with banks, shops, health services, government authorities, etc. A number of so called 'password managers' have been developed to assist the user in form filling and keeping track of a growing number of username and password pairs.[17] In this context, we often do not speak of identity management *systems*, but rather of more limited applications. These may be installed on the user's device, e.g. integrated in the browser, or as a service provided on a proxy server where they may be accessible to the user regardless of the device used. User-centric identity management is also a focus for many current research initiatives[18] about privacy-enhancing identity management, which seek to minimise personal data and to give the end-user control over the disclosure of such data. These privacy-enhancing mechanisms include, among others, data minimisation through anonymous communication, attribute authentication and utilization of multiple un-linkable context dependent pseudonyms.[19]

---

15 See e.g. Jøsang, A. and Pope, S., 'User Centric Identity Management', AusCERT Conference 2005. http://sky.fit.qut.edu.au/~josang/papers/JP2005-AusCERT.pdf, last visited 5 March 2007.

16 Identity is an ambiguous term and it is therefore useful to distinguish between digital (or partial) identities and the physical 'real world' entity/person. See about this distinction in Jøsang, A. and Pope, S., 'User Centric Identity Management', AusCERT Conference 2005, and Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, pp. 28-37. See also suggestions for a terminological framework for identity management in the Modinis research project, 'Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management', Consultation paper, v2.01, November 23, 2005.

17 See Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, pp. 21-24.

18 See e.g. the PRIME project and other projects referred to in footnote 5. Microsoft's recent initiative for an identity metasystem and Windows CardSpace seems to bring some of the large commercial actors more towards user-centric identity management which cater for privacy-enhancing mechanisms. See footnote 4 and references therein.

19 See in general Burkert, H., 'Privacy-enhancing technologies: typology, critique, vision', in Agre, P. E. and Rotenberg, M. (ed.), Technology and privacy: the new landscape, MIT Press, Cambridge, 1997, pp. 125-142. See also Brands, S. A., 'Rethinking Public Key Infrastructures and Digital Certificates', MIT Press, 2000, and numerous publications by Camenisch, J. http://www.zurich.ibm.com/~jca/publications.html, last visited 30 January 2007.

2.3 Examples

For the purpose of this paper we will analyse two of the most prominent examples of identity management systems: Microsoft .NET Passport and the Liberty Alliance specifications for identity management.

2.3.1 Microsoft .Net Passport

Microsoft .Net Passport was one of the first large scale identity management systems for multiple organisations. Microsoft .NET Passport dates back to 1999 and historically provided simplified access to many organisations' Internet resources. It facilitated consumers' access to numerous web sites and resources after a single authentication procedure (*single sign-on*).[20] In 2002, there were over 250 million registered accounts, which facilitated access to 69 external websites worldwide.[21] Due to privacy concerns, the European data protection authorities (i.e. the Article 29 Working Party) started enquiries on the functioning of the .NET Passport service in 2002.[22] These enquiries eventually ended in a number of requirements that had to be met by Microsoft in order to be compliant with the EU Data Protection Directive.[23] These privacy issues may have been among the reasons why Microsoft discontinued its use of

20 For further information, see Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG) 'Identity Management Systems (IMS): Identification and Comparison Study',2003, p. 125, available at http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf, last visited 18 January 2007; Oppliger, Rolf, 'Microsoft .NET Passport and identity management' Information Security Technical Report, Vol. 9 No. 1, 2004, pp. 26-34.

21 Twenty-two of these sites were based in countries which are members of the European Economic Agreement, where the Data Protection Directive is in force. See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, p. 5. The Article 29 Working Party did not specify how it counted the number of 'EEC sites', but it can be assumed that this refers to the number of websites for which national data protection law of any of the member states of the European Economic Agreement is applicable according to Article 4 of the Data Protection Directive.

22 See Article 29 Working Party 'First orientations of the Article 29 Working Party concerning on-line authentication services', 2 July 2002. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp60_en.pdf, last visited 5 March 2007.

23 The requirements addressed the lack of information given to data subjects, the value of the consent given by the data subjects, the proportionality and quality of data collected and stored by .NET Passport and further transmitted to affiliated sites, the data protection rules applied by the websites affiliated to .NET Passort, the necessity and conditions of use of a unique identifier, the exercise of the rights of the data subjects and the security risks associated with the centralised architecture. See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, pp. 6-11

.NET Passport for sites outside the Microsoft domain in 2003.[24] Microsoft has lately exchanged the established name with 'Windows Live ID', which seems to have put an end to .Net Passport for Microsoft.

The renaming of .NET Passport into Windows Live ID may indicate that Microsoft wishes to renew its approach to identity management. Since Windows Live ID is not designed as a multi-organisation system, it falls outside the scope of this paper. Instead, we will concentrate on the .NET Passport as it was originally designed, i.e. facilitating identity management for a multiplicity of services on the Internet.

2.3.2 Liberty Alliance

The second example to be examined is the framework for identity management developed by the Liberty Alliance Project[25] ('Liberty'). The Liberty Alliance Project was established in 2001, as a counterweight to Microsoft's dominance in the identity management arena. It is an industry consortium of more than 150 organisations worldwide, seeking to establish standards, guidelines and best practices for federated identity management.

Federated identity management provides a framework for multi-organisation identity management both from a technical and organisational perspective.[26] It consists both of a technology that facilitates the communication of identification data and of a network of collaborating organisations, which allows the creation of new collaborative business models. This refers to the provision of services by multiple organisations, where one site may accept a user who has been authenticated by any of a range of participating identity management service providers (*identity providers*). A popular definition of federated identity management used by, among others, the Burton Group, is 'the agreements, standards and technologies that make identity and entitlements

24 Hence, .NET Passport changed from a multi-organisation single sign-on identity management system to a single-organisation single sign-on identity management system. In its simplest form, (single-organisation single sign-on), the identity management system allows persons to access multiple applications, servers or sites which all belong to the same organisation, e.g. by employees or customers to that organisation. Multi-organisation single sign-on refers to an identity management system that allows persons to access multiple applications, servers or sites within multiple organisations. See further about this categorisation in Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, pp. 10-12. Microsoft is currently developing a new identity management selector called 'Windows Cardspace', which is scheduled to be released early 2007. See further footnote 4.

25 For an overview of the Liberty Alliance Project, visit www.projectliberty.org.

26 For an analysis of federated identity management, see Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, pp. 13-17.

portable across autonomous domains'.[27] The definition emphasises the degree of commonality that is needed for organisations to accept a user who has been authenticated by any of a range of identity providers. The network of collaborating organisations is by Liberty Alliance referred to as a *circle of trust*.[28]

Since the introduction of the concept of federated identity management by Liberty Alliance, several industry consortia and standardising bodies have been involved in the development of technical standards for federated identity management, including e.g. OASIS,[29] 'WS-*'[30] and 'Internet 2'.[31] Some of these standards were initially parallel and to some extent competitive initiatives. However, during the last years there has been some convergence.[32] Currently, several vendors offer identity management products and services based on these standards for identity federation. However, there are also other initiatives and approaches to identity management which to some extent complement or overlap with these standards.[33]

This paper uses the Liberty Alliance specifications as an example of federated identity management. It should be noted that Liberty is merely a consortium issuing specifications and does not provide products or services directly to the public. Hence, it will not directly manage companies' compliance with data protection laws. Nevertheless, Liberty has acknowledged that compliance with data protection law is fundamental for any successful implementation of the specifications. Liberty claims that security and data protection concerns have been taken into account when developing the technical standards.[34]

27 Burton Group, Directory and Security Strategies Research Report, 'Towards Federated Identity Management: The Journey Continues', August 2003.

28 See Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23, 2005.

29 OASIS (Organization for the Advancement of Structured Information Standards). www.oasis-open.org.

30 WS-* comprises a number of standards developed by a few but very large companies, i.e. IBM, Microsoft, BEA, RSA and Verisign.

31 See http://www.internet2.edu/.

32 For example, the SAML 2.0 specification has since its ratification in March 2005 by OASIS been the preferred standard for identity federation in Liberty. More recently, there have been signs of a possible convergence also between Liberty Alliance Web Services Framework and WS-*. See Kirk, J., 'Liberty Alliance, Microsoft discuss identity protocols', Networked World, 10 January 2007. http://www.networkworld.com/news/2007/011007-liberty-alliance-microsoft-discuss-identity.html?page=1, last visited 7 March 2007.

33 See e.g. OpenID, http://openid.net/. See also Microsoft Windows CardSpace, described in footnote 4.

34 See Liberty Alliance Project, 'Privacy and Security Best Practice', version 3.0 November 12, 2003.

However, it is difficult to ascertain to what degree the specifications actually fulfil security and data protection requirements.[35]

While the technical architecture is of importance for how data will be processed, it is also crucial how collaborators actually choose to implement the specifications and how they administer responsibilities within a network of collaborators. Consequently, Liberty has provided some guidance on possible contractual frameworks and operational rules for adopters of the specifications.[36]

2.3.3 Rationale for the choice of examples

The Microsoft .Net Passport system and the Liberty Alliance specifications are both useful as examples for the analysis of data protection issues of identity management.

The .NET Passport case is, so far, the only instance where data protection authorities have put identity management systems under scrutiny. It is therefore a natural starting point for any analysis of the data protection aspects of identity management. This is further supported by the Article 29 Working Party's general approach to identity management, where it emphasised that the conclusions reached 'should be considered as being of general application to any online authentication system when dealing with similar issues'.[37] The discontinued use of .NET Passport as the intended universal identity management system for the Internet can therefore be studied as an example of the problematic aspects of such systems, and these experiences may provide useful insight for future identity management systems. We will therefore study the lessons learned from the failure of the original .Net Passport solution, in order to draw some conclusions for future and emerging identity management collaborations.

The Liberty framework is suitable for a legal analysis because it is sufficiently coherent and since it provides rich examples of implementations at business level, where legal issues need to be addressed. Moreover, Liberty Alliance

35 There is a lack of independent literature, since most of the material about Liberty is issued by the project itself. For the purpose of this paper, we have reviewed the available information with a view to providing an independent analysis. However, since the authors' main field of competence is law, we need to base our analysis on the available technical details as provided by Liberty.

36 See Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23, 2005.

37 Article 29 Working Party 'Working Document on on-line authentication services', January 2003, p. 14.

is an influential actor, not least due to its rather broad membership basis.[38] By focusing on the Liberty framework we seek to avoid the likely confusion that may result from the numerous possibilities of combining overlapping and partly converging standards and approaches.[39] However, the legal issues raised in this paper are of general nature and will thus apply analogously – subject to some technical adjustments – to other approaches to identity management.

Nevertheless, the chosen example cases have their limitations, since they are not easily comparable. We can not provide a valid comparison of the clearly distinguishable .Net Passport system, which was implemented in a singular way, with the Liberty Alliance *framework*. The latter is in essence is not a system, but a set of open technical standards which in principle can be implemented by any network of organisations. Comparing these two examples would be like comparing a once existing building, which has collapsed, with a set of technical standards and building elements, which can be combined in numerous ways. It is possible to say that the collapsed building was not fit, due to static problems. However, the question does not make sense for the building blocks, which can be assembled in a more or less stable way. We can thus not state whether Liberty Alliance is compliant with data protection law, since this essentially depends on the implementation of the specifications.[40] Instead, the article's objective is to discuss the legal requirements for a compliant implementation of these specifications.

2.4 Terminology

The term *federated identity management* has connotations to the constitutional and international law of federal states like the USA or Germany. The concept refers to a group of states united with one government which decides

38 See http://www.projectliberty.org/liberty/membership/current_members, last visited 9 March 2007.

39 For example, a recent paper mentions the following alternative combinations: (i) CardSpace authentication with SAML & CardSpace SSO, as opposed to (ii) OpenID with CardSpace Authentication & SAML-SSO. The paper concludes as follows: 'Notwithstanding the unique capabilities, there is a significant degree of duplication of functionality between the various systems. Convergence between the systems would eliminate such duplication and result in a simpler identity landscape.' See Ping Identity White Paper 'Internet-Scale Identity Systems: An Overview and Comparison' http://www.pingidentity.com/resources/90, last visited 7 March 2007.

40 Cf Article 29 Working Party 'Working Document on on-line authentication services', January 2003, p. 12: 'The Liberty Alliance protocol is neutral regarding data protection. It allows compliance with the Directive but certainly does not require it and no measures are taken concerning enforcement'. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf, last visited 5 March 2007.

foreign affairs, defence, etc., but in which each state can have its own government to decide its own affairs.[41] The Liberty Alliance seems to have adopted the notion of federation in order to create an explicitly new notion.[42] Arguably, the notion of federation in identity management is much more limited than in constitutional law. Organisations who utilize federated identity management do not form anything that resembles a 'federal government'. Their cooperation seems to be rather limited to jointly facilitating single sign-on within a contractual framework.

A *circle of trust* is defined as 'a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment'.[43] The term circle of trust is in itself interesting, since the use of the word *trust* seems to indicate that one or more trustors trust one or several trustees.[44] One might think that this referred to the end-user as a trustor and his chosen service providers as trustees. However, Liberty seems to use a different perspective, focusing primarily on the 'trust' between service providers. The end-user is expected to make a selection amongst the service providers in the circle of trust, i.e. it is anticipated that the end-user may *not* trust some providers in the circle. Hence, the end-user's trust is not relevant for the delimitation of the circle of trust. Instead, it is established as a cooperation of service providers. Due to the multiplicity of potentially involved parties in federated identity management, it is questionable whether trust is a useful concept to denominate a cooperation of service

41 See, e.g. Friedrich, C. J. 'Nationaler und internationaler Föderalismus – Theorie und Praxis', Pol. Vierteljahresschr. 5 (1964), p. 154.

42 The .NET Passport solution was normally not referred to as federated.

43 See the Liberty Glossary, https://www.projectliberty.org/specs/draft-liberty-glossary-1.3-errata-v1.0.pdf.

44 In addition to this relation-based trust, there is also the concept of institution-based trust, based on the 'trust in the system'. The latter type of trust may be relevant with respect to the issue of whether users will trust an identity management system as such. However, when selecting individual service providers e.g. for single sign-on, we need to apply a relation based concept of trust. We are basing our definition of trust on Gambetta, D., 'Can We Trust Trust?' In Gambetta D. (ed.): Trust: Making and Breaking Cooperative Relations, pp. 213-238, Basil Blackwell, Oxford, 1990, whose definition is well established within trust management, see e.g. Jøsang, A., Keser, C. and Dimitrakos, T., 'Can We Manage Trust?' Proceedings of the 3rd International Conference on Trust Management, iTrust 2005, LNCS 3477, pp. 93-107, Springer, 2005. On the notion of institution-based trust, see e.g. McKnight, D. H., Chervany, N.L., 'What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology', International Journal of Electronic Commerce 6 (2002), pp. 35-59; Pavlou, P. A., 'Institution-based Trust in Interorganisational Exchange Relationships: The Role of Online B2b Marketplaces on Trust Formation', Journal of Information Systems 11 (2002), pp. 215-243.

providers. Trust can be defined as the *subjective probability* by which an actor, the trustor, expects that another entity, the trustee, performs a given action on which its welfare depends.[45] Being 'trusted' is thus an attribute that is primarily valid for a specific relation between a trustor and a trustee, and which is not necessarily transitive: Anyone who has a perspective or opinion different from the trustor may or may not choose to trust the same person or organisation. Hence, it would have been clearer to speak of a *circle of cooperation* instead of circle of trust. This would also elucidate the need for a well-defined basis for this co-operation, e.g. in a contract. The term circle of trust could then have been reserved for those service providers actually trusted by the end-user. Another interesting terminological suggestion is *authentication domain*,[46] which however does not sufficiently denote the possibility of covering multiple organisations. In any case, it is not the objective of this paper to suggest alternative wordings for the concepts developed by Liberty. Concomitantly, in the remainder of this paper we will employ the term circle of trust as it is understood by Liberty.

2.5 Identifying risks

The idea of having identity information communicated freely between organisations raises concerns about privacy and data protection risks. If users are to trust a circle of trust, they may want to verify that they do not risk having their on-line behaviour monitored by an unknown number of organisations, which may utilize personal information for widely varying purposes. Hence, users may be interested in knowing which of the collaborators can access their personal information, how the flow of information is controlled and whether collaborators can collect personal information to create user-profiles which span across multiple domains. Such systems need to cater for the inherently conflicting interests of users who on the one hand wish to access on-line resources from different organisations without unnecessary bureaucratic and practical burdens, but who may not want to be monitored and profiled by all of these organisations. Moreover, even for users who do not care about their privacy, European data protection law regulates the use of personal information, limiting the use of personal information in a cross-organisational setting.

45 See supra footnote 46 on relation-based trust.

46 Sun Java Systems Access Manager 6 2005Q1 Federation Management Guide, Chapter 1 Introduction to the Liberty Alliance Project, http://docs.sun.com/source/817-7648/intro.html, last visited 26 January 2007.

Thus, identity management systems need to respect the privacy of their users and comply with data protection law.

The organisations forming a circle of trust will need to manage the risks arising from the set-up and operation of the identity management system. Risk management consists generally of coordinated activities to direct and control an organisation with respect to risks.[47] For an identity management system, which involves a variety of collaborators and possible users, a risk management process should take into consideration the risks for all of the different stakeholders. The aim is to enhance the potential benefit of the system by managing and balancing those risks. A risk analysis would thus need to take into consideration that the risk picture depends on the perspective: For an end-user, the risk of utilizing an identity management system may e.g. involve the possibility of being monitored and profiled by many different organisations. For a service provider, the risk of using an identity management system may e.g. involve the loss of reputation (and customers) in case of perceived data protection problems. A service provider may even consider a potential liability for infringements of data protection laws. All these perspectives need to be considered in a risk analysis. The notion of legal risk analysis implies that both legal and other risks are considered and managed in an integrated process.[48] In this paper, we analyse data protection issues without doing a formal legal risk analysis. Nevertheless, the current paper could be utilized as a basis for a more formal legal risk analysis in a specific case.[49]

2.5.1 Choice of identity provider

One of the key differences between Liberty and .NET Passport is the number of identity providers foreseen in the respective identity management system.

47 Definition 3.1.7 of ISO/IEC Guide 73:2002 'Risk management – Vocabulary – Guidelines for use in standards' ISO/IEC 20002.

48 See, e.g. Mahler, T. and Bing, J., 'Contractual Risk Management in an ICT Context – Searching for a possible Interface between Legal Methods and Risk Analysis', Yulex 2006, NRCCL 2006, pp. 117-138.

49 A legal risk analysis is a part of a risk management process. The analysis would cover the identification, estimation and evaluation of risks for a particular stakeholder as well as a systematic search for possible treatment measures which may reduce the risk values. Such an analysis may e.g. be based on the Australian/New Zealand Standard for Risk Management. For an example of a case study in which legal risk management was applied, see Mahler, T. and Vraalsen, F., 'Legal Risk Management for an E-Learning Web Services Collaboration.' In: Kierkegaard, S. M. (ed.): Legal, privacy and security issues in information technology - volume 1. Proceedings of the First International Conference on Legal, Privacy and Security Issues in IT (LSPI), held in Hamburg, Germany, 30.04.2006 - 02.05.2006. Oslo: Complex 2006 (3), pp. 503-523.

.NET Passport was based on one single centralised identity provider, while Liberty's specifications cater for multiple identity providers. Although there may be benefits with a centralised identity provider with regard to maintenance and cost, centralisation also implies concentration of personal data, which may result in an attractive target for attackers.[50] Centralised systems may also facilitate the possibility for the identity provider to merge the user profiles at the different service providers. Federated identity management, on the other hand, foresees the possibility of choosing among multiple identity providers (e.g. a bank or a telecom operator). The user may consent to two or more service providers within the same circle of trust to federate his partial identities. There is not necessarily a single point of failure in federated identity management and the user may have more control over his identities. However, there is also the implication that the user has to take more responsibility for the management of his own partial identities. It seems to be one of the key challenges of identity management systems to provide users with sufficient and relevant information that enables them to make informed decisions regarding the use of the system. Incomplete information and lacking transparency were amongst the main deficiencies found by the Article 29 Working Party in the .NET Passport case.[51] These issues will be analysed further in section 4.

2.5.2 Use of identifiers

Another critical matter identified by the Article 29 Working Party regarding the .NET Passport service was the necessity of and conditions for using a unique identifier. .NET Passport used a single identifier for each user, the Passport Unique Identifier ('PUID'), which is generated at registration and persists for the life of the account. The PUID was not based on any information provided by the account holder and there was no information about the account holder that could be derived from the PUID.[52] The Working Party's principal concern was that use of the PUID would enable participating sites to share information about .NET Passport users and build user profiles. Even though the contracts

50 Article 29 Working Party 'Working Document on on-line authentication services', January 2003, pp. 11. On a far-reaching approach to transfer the principle of distributed security to cybercrime law, see Brenner, S. W. and Clarke, L. L., 'Combatting Cybercrime Through Distributed Security', in: Kierkegaard, S. M. (ed.): Legal, privacy and security issues in information technology - volume 1. Proceedings of the First International Conference on Legal, Privacy and Security Issues in IT (LSPI), held in Hamburg, Germany, 30.04.2006 - 02.05.2006. Oslo: Complex 2006 (3), pp.113-135.

51 See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, p. 15.

52 For further details, see ibid, pp. 9-10.

between Microsoft and affiliated sites prohibited selling PUID registers to third parties or cross-site linking, the Article 29 Working Party perceived this as a risk since such disclosure was technically possible.

Identity federation based on Liberty specifications has avoided the use of one unique identifier for each user. Instead Liberty uses so called 'opaque handles' or 'name identifiers', which are unique identifiers used to provide a link between the user and his two federated identities. The same handle is not meant to be used to federate any other partial identities belonging to the user. Similar to the PUID in the .NET Passport service, the opaque handles are pseudonyms which do not reveal any information about the user to any third parties. The handle only gives meaning to the service or identity providers in relation to the related user, and the user should normally not have access to it.[53] Although the default situation in the specifications is that data on users should be linked only between pairs of sites, it remains to be seen whether this is enough to ensure a sufficient level of data protection. Even the Article 29 Working Party stresses that it is 'necessary to continue considering this issue from the data protection perspective, in particular concerning the technical possibility of sites sharing personal data of user without his consent'.[54]

Identity management systems may challenge one of the key mechanisms utilised to enhance data protection, i.e. the compartmentalisation of an individual's personal data into separated data sets for the different roles a person has in society. Historically, data protection law has developed as a reaction to the introduction of computer systems e.g. in public administration in the 1960s.[55] In recent decades, the private sector has also become very data intensive and there has been particular concern about these organisations' ability to match data from different sources and sectors. One of the most effective means to avoid translucent citizens and 'big brother' scenarios has been the compartmentalisation of the individual's sphere into many roles, and the

53 For more information, see Liberty Alliance Project, 'Liberty ID-FF Architecture Overview', version 1.2-errata-v.1.0. http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

54 See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, p. 12. See also the controversial report from LSE which is critical to the direct utilization of the Liberty specifications for government-built identity management: The Identity Project – An assessment of the UK Identity Cards Bill and its implications, LSE, version 1.09, June 27, 2005. http://is2.lse.ac.uk/IDcard/identityreport.pdf.

55 See e.g. Westin, A. 'Privacy and Freedom', Atheneum, New York, 1967, chapters 7 and 12; Abel, R.-B. 'Zur Geschichte des Datenschutzrechts', in: Roãnagel (ed.), Handbuch Datenschutzrecht, 2003, p. 194; Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, pp. 93-100.

accumulation of data about those roles in separate data collections. The key factors for this compartmentalisation are the use of context specific identifiers and the corresponding avoidance of multi-purpose identifiers.[56]

2.5.3 The sharing of personal information through web services

An important part of the Liberty Alliance specifications is the Web Services Framework.[57] Basically, Web Services offer a standard external interface to internal computer systems, allowing more automated interactions between computer systems.[58] The aim of Web Services is to facilitate collaboration among web sites and open up for new functionalities and business models. In particular, it is envisaged that personal data relating to data subjects may be disclosed between services providers. For example, it may be convenient for the data subject to allow a service provider to collect data directly from another service provider instead of having to provide this information himself. The Liberty Web Services Framework caters for such disclosure of end-user attributes between service providers who participate in a circle of trust based on the Liberty Identity Federation Framework.[59] However, such sharing may be perceived as a risk from the point of view of the end-user, and needs to comply with a number of legal requirements from data protection law. These will be addressed in more detail in the remainder of this paper. Section 3 will address how controllers can collaborate with respect to the processing of personal data and Section 4 will focus on the communication between the service providers and the end-user.

2.5.4 Microsoft .Net Passport and Liberty Alliance

As mentioned above, it is not feasible to provide a full comparison between .Net Passport and Liberty Alliance, due to the inherent openness of the Liberty framework. Nevertheless the following table summarizes some of the key

56 See Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, p. 18. See also the Article 29 Working Party 'Working Document on E-Government', 8 May 2003, which analyses utilisation of unique or sector based identifiers in several EEA Member States for access to on line administrative services. An analysis of the Personal Identification Number in Norway can be found in the Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, pp. 75-77.

57 For an overview, see Liberty ID-WSF 'Liberty ID-WSF – a Web Services Framework', 2004, http://www.projectliberty.org/liberty/content/download/390/2729/file/Liberty_ID-WSF_Web_Services_Framework.pdf.

58 See e.g. Clarke, R., 'Identity Management', Xamax Consultancy, March 2004, p. 1.

59 See 'Liberty ID-WSF – a Web Services Framework', 2004, pp. 10-12.

characteristics of the two schemes. The controller responsibility and the contractual framework will be discussed further in section 3.

	Microsoft .NET Passport	**Liberty Alliance**
System	Single system. Implemented in a singular way by Microsoft.	Open specifications. Can be implemented in various ways within multiple different systems.
Single sign-on	Previously multi-organisation single sign-on. Since 2003 single-organisation sign-on.	Depends on implementation, supports multi-organisation single sign-on.
Choice of identity providers	Microsoft was the only identity provider.	Allows for several identity providers so far as they are accepted by the service provider.
Identifiers	Unique PUID per user.	Unique handle per user per federated pair of site.
Responsible controller	Microsoft and service providers were single data controllers.	Controllers or processors? – Service providers within a circle of trust become data controllers «at the time users visit their sites», according to Article 29 Working Party. – However, according to the Liberty Alliance, it is possible that some service providers may act as processors.
Contractual framework	Contract between Microsoft and service provider.	Implementation-dependent – According to Article 29 Working Party, a «contract between every site in a circle of trust». – However, depending on the type of implementation, other models may be possible. For example, it may be sufficient that every participating service provider has a contract with one party, which organizes and administrates the circle of trust.

Table 1 – Key characteristics of .Net Passport and Liberty Alliance framework

3 Roles and responsibilities of collaborators under data protection law

The previous section illustrated the impact the technical specifications have on the end-users' privacy. If the system is perceived as privacy infringing, this will endanger the reputation of the involved service provider, which may lead to a loss of profits in the long run. Thus, privacy deficiencies may have negative consequences both from the perspective of end-users and service providers. However, for a service provider, this is also a matter of compliance and possible legal sanctions. Such legal risks depend on the utilized technical specifications, as well as on the organisational and contractual framework which specifies the operating rules and the terms for the collaboration.

In the following subsections we will study the roles and responsibilities set out in the Data Protection Directive and the E-Communications Directive and how the Data Protection Directives apply to identity management. Section 3.1 provides an introduction to data protection law. Subsequently, Section 3.2 analyses the difficulties of assigning responsibilities to parties who process personal data in collaboration with others. Finally, Section 3.3 discusses how the fundamental aspects of the federated processing of personal information should be laid down in a contract between the collaborators.

3.1 European data protection law

The objective of this section is to introduce European data protection law as the relevant legal framework for multi-organisation identity management as far as personal information is concerned. Data protection in Europe is governed by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the Data Protection Directive) and Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter the E-Communications Directive).

The aim of the Data Protection Directive is to reconcile privacy protection with the free flow of trade.[60] In particular, it sets out requirements for lawful processing of personal data and requires that specific controls be afforded to sensitive data.[61] The E-communications Directive provides specific rules for the processing of data related to service provision over electronic communications

60 See Data Protection Directive, Articles 1(1) and (2) and recital 3.
61 See Data Protection Directive, Article 8.

networks (e.g. traffic and location data) and the information security requirements in such networks.

The term *personal data* is defined in the Data Protection Directive, Article 2, as 'any information relating to an identified or identifiable natural person'. An 'identifiable person' is one who can be identified, 'directly or indirectly, within a reasonable time, considering the necessary effort taking account of all the means likely reasonably to be used'.[62] This includes, in particular, identification by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. An example of personal data would be 'Billy accessed resource X at time Y'. This example can be split into 1) the non-personal data 'someone accessed resource X at time Y' and 2) the identifier[63] 'Billy', which is linked to the former data.[64] If we permanently and irrevocably remove the identifier, and if the person can not be identified from the context,[65] the data is anonymous and data protection law is not applicable.

Since the Data Protection Directive and the E-communications Directive provide for harmonisation[66] of data protection laws in the EU and the European

62 Data Protection Directive, recital 26. See further Beyleveld, D., Townend, D. 'When is personal data rendered anonymous? Interpreting recital 26 of Directive 95/46/EC' (2004) Med. L. Int. 6(2) 73; Casabona, C. M. R. 'Anonymisation and pseudonymisation: the legal framework' In: Beyleveld, D. (ed.) et al., Implementation of the Data Protection Directive in relation to medical research, Vol. 1, London 2004, pp. 33-44.

63 A particular type of identifiers is explicitly addressed in Data Protection Directive's Article 8 number 7, according to which 'Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.'

64 Of course, it may be possible that 'Billy" is a pseudonym. Whether the data would be considered as personal, will depend on whether it is possible to identify the person behind the pseudonym 'Billy". Notably, the latter may differ from one actor to another. This is to say that in an identity management system, some service providers may be in a position identify the person behind the pseudonym, while others are left with the pseudonym. This implies a number of uncertainties for those service providers who only have access to pseudonyms: The law is not very specific about how pseudonymous data are to be evaluated, and there are in general few court or other decisions which could give guidelines about pseudonymous data. This uncertainty is further enhanced by the fact that the spectrum of choice between personal data and anonymous data is wide, see Clarke, R., 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice', presented at User Identification & Privacy Protection Conference, Stockholm 14-15 June 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html, last visited 30 January 2007.

65 In our example, contextual identification could happen if we assume it is known that resource X was only available to Billy at time Y.

66 The Directives, qua directives, require the Member States to implement the Directives' provisions in national law. It is important to note that the applicable national laws are the point of departure for establishing the rights of the data subjects and the obligations of control-

Economic Area (EEA),[67] our analysis of these instruments reflects the legal situation in the EU/EEA Member States.[68] Despite there being some national differences, the most important rules in data protection law can at a meta-level be expressed as a number of basic principles, which can be found in most international and national data protection instruments and laws.[69] The following are of particular importance in the context of identity management:

- *Fair and lawful processing*: According to the Data Protection Directive, Article 6 (1), personal data must be processed fairly and lawfully. The requirement of lawful processing implies that it may only be processed if certain conditions are fulfilled, e.g. if the person has given his or her consent or if the processing is necessary for a legitimate reason as specified in data protection law.
- *Purpose specification*: Personal data must be collected for specified, explicit and legitimate purposes and not further processed for other purposes.
- *Minimality*: The collection and storage of personal data should be limited to the amount necessary to achieve the purpose(s). Purpose specification and minimality are problematic in a setting where different collaborators pursue differing purposes.
- *Data subject participation and control*: Persons should be able to participate in the processing of data on them and they should have some measure of influence over the processing.
- *Disclosure limitation*: The data controllers' disclosure of personal data to third parties shall be restricted, it may only occur upon certain conditions. This principle is based on limiting the number of parties who can access personal data, which is not easily compatible with collaborative procedures. The distinction between authorized parties and 3rd parties is not trivial in a collaborative setting.

---

lers. The main criteria for determining the applicable national law is where the controller is established, cf. Article 4 of the Data Protection Directive. See further Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, pp. 49-52.

67 The EEA consists of the EU Member States including the EFTA Member States Norway, Iceland and Liechtenstein.

68 However, according to an evaluation of the implementation of the Data Protection Directive, there are some divergences on how the Data Protection Directive's provisions have been implemented. European Commission, 'First report on the implementation of the Data Protection Directive', COM (2003) 265 final. http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm.

69 Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, p. 46.

- *Information security*: The data controller must ensure that personal data is not subject to unauthorised access, alteration, destruction or disclosure. This is challenging when the security obligation is shared between several controllers, since the achieved security level may depend on the weakest link.[70]

As is evident from the issuing date of the Data Protection Directive, its drafters were not able to address the issues of the then emerging Internet. Hence, the management web data in general and of electronic identity information in particular, were not addressed. We therefore need to rely on newer sources. In this respect, reference will be made to the recommendations by the Article 29 Working Party ('the Working Party').[71] In the absence of other authoritative sources of law (e.g. clear legal provisions, case law or practice by the supervisory authorities) the recommendations by the Working Party should be given considerable weight when determining the data protection law applicable to multi-organisation identity management systems.

3.2 Collaboration and responsibilities

When personal data is processed in collaboration with others, it may be difficult to administrate the liability and to jointly ensure compliance with data protection law. One of the key decisions in analysing data protection responsibilities is determining the status of the involved parties. The following subsections will therefore first introduce the roles that are available in data protection law (Section 3.2.1), then consider how the collaboration between actors holding these roles is understood in the law (Section 3.2.2) and finally discuss how these questions can be applied to identity management systems (Section 3.2.3).

3.2.1 Roles

Data protection law contains four distinct roles, which may be assumed by a participant involved in multi-organisation identity management: 1) The controller is responsible for the processing of personal data. 2) The processor processes personal data on behalf of the controller. For the purpose of this

70 See Arce, I., 'The weakest link revisited [information security]', Security & Privacy Magazine, IEEE, vol.1, no. 2, pp. 72- 76, Mar-Apr 2003.

71 The Working Party is an independent European advisory board on data protection comprised of representatives from the supervisory authorities in the EEA Member States. The Working Party's tasks, which are described in Article 29 and 30 of the Data Protection Directive and in Article 15 in the E-Communications Directive, include contributing to the uniform application of the provisions in the two Directives.

paper we can disregard the two remaining roles, i.e. 3) the 'public electronic communications network provider'[72] and 4) the 'public electronic communications service provider',[73] defined in the E-communications Directive. Network operators merely provide communication services and are normally not to be regarded as controller of any personal data *contained in* a transmitted communication.[74] In the following sections, we will merely focus on the roles contained in the Data Protection Directive, i.e. controllers and processors.[75]

Article 2(d) of the Data Protection Directive defines the controller as the natural or legal person who determines the purposes and means of the processing of personal data. In other words, you will be a controller if the processing of personal data is undertaken for your benefit and you decide what personal data should be processed and why. The processor, on the other hand, is defined in Article 2(e) as the person who processes personal data on behalf of the controller. A common example is where an organisation appoints a third party to provide IT services to that organisation on an outsourcing basis. In

72 The public electronic communications network provider operates the public electronic communications network, cf. Article 2(a) of the Framework Directive. The term public electronic communications network is defined in Article 2(a) of the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services ('Framework Directive'). This role captures the operators of the relevant network infrastructure, regardless of the technology used. The E-communications Directive applies only to 'public' electronic communications networks, which excludes networks that are not made available wholly or mainly for provision of electronic communications services to the public (e.g. enterprise networks and other internal systems).

73 The public electronic communications service provider offers electronic communications services to the public. An electronic communications service is defined in Article 2(c) of the Framework Directive as 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting'. This excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. It also excludes information society services, as referred to in Article 1 of Directive 98/34/EC and the Electronic Commerce Directive 2000/31/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. It is possible for entities to operate both as public electronic communications network provider and public electronic communications service provider, e.g. traditional telecommunications operators may both provide the network infrastructure and services on those networks to the public.

74 However, the operator, as a communication network or service provider, will normally be considered a controller for the processing of the additional data necessary for the operation of the service (e.g. traffic data and location data), see Data Protection Directive, recital 47.

75 Determining the roles of the parties is also significant with regard to the rules on applicable law. The main rule in Article 4 in the Data Protection Directive is that the applicable law in respect of the processing will be that of the country of establishment of the controller, not the processor. See further Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, Sections 3.1 and 4.3.

this circumstance, the organisation will be the controller (since it has decided to appoint the IT service provider) and the IT company is the processor, i.e. it acts on the instructions of the controller.

The obligations set out in European data protection laws are primarily placed on the controller. Processors are generally not directly subject to data protection laws in respect of processing undertaken in their capacity as processor. However, national laws based on Article 17 of the Data Protection Directive require controllers to choose a processor providing sufficient guarantees in respect of technical and organisational security measures, and to 'ensure compliance' with those measures. The controller is also obliged to have a contract in place with its processors which stipulates that the processor shall only act on instructions from the controller. It follows from these requirements that if the controller chooses to delegate data processing to a processor, the controller will, as a point of departure, remain primarily liable for the processing carried out on its behalf.[76]

Hence, the key to identifying roles and responsibilities is to map the roles in identity management schemes[77] with those available in data protection law (primarily controller and processor). However, when attempting to map these roles one will soon realise that there is no direct connection between them. As a point of departure, the Article 29 Working Party has suggested that each participant in an identity management scheme is to be considered a controller in respect of their own processing operations.[78] Consequently, the Working Party considered Microsoft as controller with regard to the authentication service in .NET Passport, whereas the participating sites were controllers with regard to their own customers. Following this reasoning, the point of departure regarding identity management using Liberty specification would be that any service provider in a circle of trust will be the controller of the personal data relating to its customers and/or employees.

However, the complexity of collaborative relations in identity management systems may make it a difficult task to clearly define who is a controller.

---

76 In case of any unlawful processing by the processor (in breach of the controller – processor contract which causes damage to any other person), it is likely that the controller would remain primarily liable due to its on-going obligations to ensure compliance by the processor. See Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, p. 26.

77 In .NET Passport the main roles are the data subject/user, authentication provider and the service provider, while in Liberty the main roles are the principal (the data subject/user), the identity provider, the service provider and the attribute provider.

78 Article 29 Working Party 'Working Document on on-line authentication services', January 2003, pp. 9 and 12.

The Liberty Alliance even envisages that the controller may change from one data-processing operation to another, even within one information system.[79] Due to the agnostic nature of the Liberty framework as regards participants' roles and responsibilities under the Data Protection Directive, it is understood by Liberty that any Liberty-defined participant may be acting in the capacity of a processor at any given time.

We may also ask what role and requirements apply to designers of the technical specifications for identity management. The Article 29 Working Party addressed this issue in its dialogue with Microsoft and concluded that '[b]oth those who design and those who actually implement on-line authentication systems (authentication providers) bear responsibility for data protection aspects, although at different levels'.[80] Placing responsibility on designers may seem like an attempt to adopt a pro-active approach to the data protection issues raised by identity management. However, it is not clear on what ground such a responsibility is based, since the designer of an identity management system is neither a data controller nor a data processor. Nevertheless, one should note the focus on systems designers in recital 30 of the E-Communications Directive: 'Systems for the provision of electronic communications networks and services should be *designed* to limit the amount of personal data necessary to a strict minimum' [italics added]. Consequently, while designers are required to take data protection issues in to consideration when developing the technical specifications, it is the organisations that implement the specifications and provide services to data subjects that are the prime subjects of data protection law. These organisations' compliance with data protection law will be dependent, of course, on the technical specifications and – perhaps even more importantly – on the way they choose to implement the specifications. Successful implementation, however, requires that the parties are aware of their role under data protection law and are able to administer their responsibilities in an identity management network.

3.2.2 Collaboration between controllers and processors

From an organisational perspective there are different degrees of collaboration between organisations. A very limited collaboration may consist of the mere occasional exchange of information; a more advanced collaboration may involve the sharing of some responsibilities in selected aspects; a full collaboration

79 See Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, p. 15.

80 See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, pp. 14-15.

would entail the sharing of all responsibilities. This degree of collaboration has consequences for the way data protection law regulates the collaborative processing of personal data.

Conceptually, there seem to be different levels of collaboration between multiple participants. Figure 3 depicts different variations in the relations between controllers and processors.

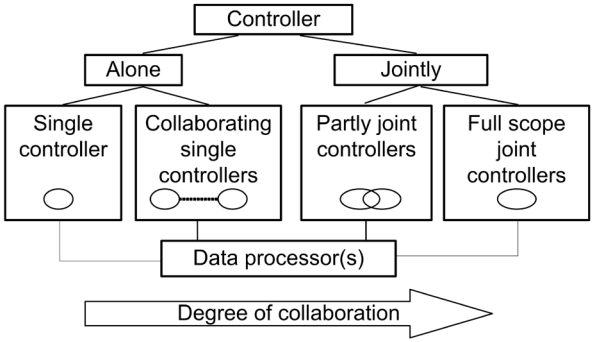


Figure 3 – Collaboration between controllers

A collaboration of organisations processing personal data will essentially involve a network of controllers and processors. One or more processors may handle personal data on behalf of one or several controllers. This controller collaboration deserves to be analyzed in more detail.

Article 2 (d) of the Data Protection Directive recognises that the controller can act either alone or jointly with others. The controller is defined as 'the natural or legal person, public authority, agency or any other body which *alone or jointly with others* determines the purposes and means of the processing of personal data' [italics added]. However, reality seems to be more complicated. In fact, a single controller may have some degree of collaboration with others, without controlling the data jointly. And we can even think of different degrees of jointly controlling data. These differences will be analyzed in the following sections.

In its simplest form, there may be controllers who have no relationship whatsoever with the other controllers. Secondly, many controllers do collaborate with other controllers without being joint controllers. This will be the case if the collaborating controllers do not make any joint decisions about the means and processing of personal data. An example would be the communication of personal information between a travel agency and a hotel, which

exchange personal information, but process it separately. It is submitted that this type of collaboration is the most relevant and typical for multi-organisation identity management.

The remaining two types of collaboration involve controllers who act jointly. The concept of joint controllers has, to our knowledge, been scarcely addressed in court cases,[81] legal research[82] and legislative documents.[83] Joint controlling is sometimes referred to as 'data processing in information pools fed by several controllers'.[84] Although the Data Protection Directive provides for having joint controllers, there is no mention of how this organisational

81 In a recent case decided by the Norwegian data protection tribunal (PVN-2005-11) regarding an automated road toll system, the data protection authority had decided that the public road authority and the respective private toll collecting operator were joint controllers. The road authority's role was to specify the automated road toll system and to issue guidelines for the processing of personal data. It was not disputed by the parties that they were, in fact, joint controllers, and this question was thus not decided upon by the tribunal, see http://www.personvernnemnda.no/vedtak/2005_11.htm.

82 The rules and practices of being a joint controller in the UK, Spain and Norway were analysed by the Legal-IST project in Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, pp. 42-43. The analysis shows that there are differences with regard to how multiple controllers can interact with each other, with some of the models described above being more readily recognised in certain jurisdictions than others. This is particularly the case with respect to the notion of joint controllers and to what extent a network of organisations with a very loose organisational structure would be recognised as data controller, even if it is not considered a legal entity. While the Spanish and the Norwegian data protection law seems to be very similar to the relevant provisions in the Data Protection Directive, the UK Data Protection Act 1998, in contrast, defines a controller as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed'. The notion of 'in common' is not to be found in the Data Protection Directive, but derives from English property law which has been developed through case law over the past couple of centuries. In contrast to the two other jurisdictions, where little guidance is given by the respective data protection authorities on this issue, the UK's data protection authority (the Office of the Information Commissioner) has provided guidance on the interpretation of English law; see Office of the Information Commissioner 'Data Protection Act – Legal Guidance', Version 1, p. 16. http://www.dataprotection.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf.

83 The analysis from the Legal-IST project has raised the general question of how collaborations of data controllers should be regulated de lege ferenda. In a recent review of the Norwegian Data Protection Act carried out by law professors Dag Wiese Schartum and Lee A. Bygrave, the issue of collaborating controllers is considered as a matter to be regulated by Parliament when updating the act in the near future, cf. Schartum, D. W. and Bygrave, L. A., 'Utredning av behov for endringer i personopplysningsloven', Justis- og Politidepartementet, Oslo 2006.

84 Kotschy considers the use of information pools to be a more and more popular form of processing, see Kotschy, W. Commentary to Directive 95/46/EC, in Büllersbach, A. et al, Concise European IT Law, Alphen ann den Rijn, 2006, p. 33.

structure affects the controllers' rights and duties when processing personal data.[85] Joint controlling may be particularly challenging in terms of the purpose specification principle, since the controllers may whish to process personal for widely varying purposes.[86] Moreover, there seem to be significant national differences with respect to joint controllers.[87] However, at least conceptually, we can distinguish between degrees of jointly controlling the processing of personal data.

The third type of controller collaboration thus envisages that some controllers will jointly determine the means and purposes of *some of the processing operations*, while other processing operations are made separately and within the sole control of one controller. If the travel agency and the hotel in the example above use a common Internet portal for communicating with their customers, they may be considered joint controllers for those of the processing operations which are being made on the jointly controlled portal, while they could be considered separate controllers with regard to further processing carried out outside of the portal.

The fourth category includes the highest degree of collaboration. Full scope joint controllers are envisaged to jointly determine the means and purposes of all the data processing operations. This may e.g. be the case for some research projects, when two or more research institutions jointly process personal data as part of a common research project. However, if the collaboration between the organisations leads to the formation of a new entity which is positioned as a data controller, this will again be the case of a single data controller, possible involving elements of vertical joint controlling.[88]

---

85 In principle, all joint controllers will be potentially liable for infringements, i.e. the data subject could potentially bring a claim against any of them. The EU Data Protection Directive is also silent regarding the implications of joint processing with respect to for example information requirements, granting the data subjects access to own data or in notifying data protection authorities. For further details, see Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, p. 48.

86 It would probably be contrary to this principle if organisations decided to become joint controllers just to overcome difficulties with respect to sharing data between separate controllers. See in general on the purpose specification principle in Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, pp. 61-62.

87 See footnote 84.

88 By a vertical relationship we refer to cases where there is a hierarchical relation between two or more joint data controllers. This is often the case in central and local government, but may also be the case in corporations with subsidiaries. A horizontal relationship is where the data controllers are not in any hierarchical relation to each other. The data controllers in horizontal relationships will, as a point of departure, be independent and autonomous parties. This is in contrast to vertical relationships where the overlying controller has often

3.2.3 Roles in identity management systems

How do these collaborative models relate to identity management systems? Regrettably, no general answer to this question can be given here. Most identity management systems will probably consist of multiple collaborating but single controllers. However, according to Liberty it is quite possible that more than one participant could be the controller in respect of any given transaction in a federation. In particular, Liberty acknowledges the possibility that data will be transferred between participants with the transferor retaining some control over that data, which could lead to processing by joint controllers.[89]

At a practical level, the business practices in a specific identity management system need to be analysed in order to determine the level of responsibility of an individual service provider.[90] It follows from the above quoted definition of data controller that the entity who determines the purposes and means of the processing is the controller. The term 'determine' suggests that the emphasis should be on the entity or entities that have decision making power or control of the data processing. The controller does not necessarily need to have possession of the data as long as it in fact determines how and for what purposes the data is processed. If an entity merely processes data on behalf of another, this entity will be a processor under the Data Protection Directive. When data protection supervisory authorities identify the controller(s), they may not only look on how the parties have defined their roles, but on the factual exercise of control. Hence, if the data controller's responsibility has been 'delegated' to another entity, the delegating entity would still be the data controller if it still in fact has control over the means and purposes of the processing. In, summary, whether an entity is a data controller or processor in a certain data processing operation depends to a minor degree upon how the participants themselves arbitrarily

delegated responsibilities to the underlying body, but the right to instruct remains with the overlying body. In the preparatory works to the Norwegian Personal Data Act there are examples of an overlying governmental body, e.g. a ministry, being joint data controller with an underlying governmental body, e.g. a directorate. In this case the ministry will determine the paramount objectives of the processing, whereas the directorate will determine the more detailed purposes and the practical means of the processing of personal data. In the preparatory works it is suggested that the directorate should be the data controller because of its daily and more direct control of the processing. See Ot prp nr 92 (1998-1999) 'Om lov om behandling av personopplysninger (personopplysningsloven)', pp. 102-103.

89 See Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, p. 16.

90 One should note, however, that there may be divergences in the interpretation and practice of this part of the Data Protection Directive in the different EEA Member States.

define their roles and responsibilities. Much more significant are the roles they actually perform in practice within their collaboration or circle of trust.[91]

It is noteworthy that even company structures may need to be considered when determining who controls the processing of personal information in a collaborative setting. For example, in some Member States subsidiaries or associated companies are considered as separate controllers.[92] This may hinder the possibilities of merging data and achieving synergies across a corporation's offered services. It may be of great importance to consider these restrictions when collecting data, e.g. by getting consent from the data subject to merge data or, in extreme cases, by reconsidering the company structures.

3.3 Contracts about the processing of personal data

The Data Protection Directive allocates compliance responsibilities to the role that any given participant is performing with regard to the processing of the data. For the relationship between a controller and a processor, a contract is mandatory. However, the Data Protection Directive does not explicitly require joint controllers or collaborating single controllers to contractually agree on how the processing is to be carried out.[93]

Interestingly, the recommendations from the Article 29 Working Party speak a different language. The dialogue between the Working Party and Microsoft illustrates the importance of clear contractual agreements between controllers. Prior to the dialogue with the Working Party, it had been unclear to what extent Microsoft controlled the data protection practices of participating sites and which rules applied to these sites. During the discussion it was made clear that Microsoft did not control the data protection practices of participating sites but that Microsoft through their contracts imposed a number of safeguards on the participating sites. The Article 29 Working Party emphasised that '[i]t is advisable for the different players to have clear contractual agreements bet-

91 Compare, Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, pp. 15-16.

92 In both Spanish and Norwegian law the concept of an unincorporated association being the data controller is not recognised. The rationale for this requirement is that it should be possible for the data subject to hold an entity liable for unlawful data processing. In contrast, under English law, a network of organisations could be a controller, even if it is not a legal entity (e.g. it may be an unincorporated association, which would be represented by its elected committee members). See Legal-IST report D11 'Privacy – Identity Management', 4 November 2005, pp. 42-43.

93 It suffices that the sending party is legally permitted to disclose and that the receiving party is allowed to process the data.

ween them where the obligations of each party are made explicit'.[94] The legal basis for this 'advice' is highly unclear, since contracts are only mandatory for controller-processor relations, while the .NET Passport case involved collaborating controllers. However, it seems like the Working Party here has touched upon a wider issue, which deserves discussion *de lege ferenda*.[95] Contracts between controllers may indeed be an incentive for collaborators to define sound data protection practices. Moreover, the existence of contractual agreements may even simplify the monitoring of collaborative practices for data protection authorities.

The Liberty Alliance also acknowledges that a contract may be of essence for organisations providing identity management services. This is for example reflected in the definition of circle of trust as a federation of service providers and identity providers who have business relationships based on the Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.[96] Liberty envisages that the structure and nature of the contractual framework will vary depending on the scope of the circle of trust. A relatively light framework may be sufficient for identity management schemes made up of a small number of more static business partners. In more complex and dynamic schemes where participants are expected to be joining, leaving and changing roles there may be a need to establish common rules which minimise the problems of bilateral negotiations and multiple contracts with many interdependencies.[97]

4 Compliant interaction with the end-user

So far, we have analysed the inter-organisational relationships between participants in identity management with regard to identifying roles and responsibilities pursuant to data protection law. This section puts emphasis on the relationships between the collaborators and the *data subject,* i.e. the end-user

94 See Article 29 Working Party 'Working Document on on-line authentication services', January 2003, pp. 14-15.

95 The current review of the Data Protection Act in Norway has resulted in a proposed new Section 7 paragraph 4, according to which a written contract would be made obligatory for joint controllers, see the so-called 'radical proposition' in Schartum and Bygrave 2006 (above note 85), p.194. It remains to be seen if this proposal will be incorporated in a bill to the Norwegian Parliament.

96 See the Liberty Glossary at: https://www.projectliberty.org/specs/draft-liberty-glossary-1.3-errata-v1.0.pdf.

97 See further, Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, p. 6.

of the identity management services. In particular, we will analyse the information requirements under the Data Protection Directive and see how they can be fulfilled in multi-organisation identity management.

Many of the basic principles found in the Data Protection Directive seek to ensure the data subject's autonomy and informational self-determination, i.e. the data subject's possibility to determine how data on him or her are processed by others.[98] Access rights and the right to information about data processing operations are necessary pre-requisites to ensure the data subject's informational self-determination.

Identity management may involve many participants who assume different roles based on complex technologies. This may pose challenges to compliance with the information requirements. One of the Article 29 Working Party's main concerns with regard to the .NET Passport service was the lack of information about the privacy implications of taking part in and further using the scheme. Particularly, the Article 29 Working Party required that the users were provided with clear information about which parties were responsible for which data processing operations and that the users were given better choice and control with regard to disclosing information to participating service providers.

This requirement to a certain degree impedes a fully seamless user experience, since some of the 'seams' or boundaries between the service providers are legally preserved as visible. The key functionality to achieve a seamless user experience is single sign-on, i.e. the option to access resources provided by several service providers after a single authentication procedure. This means that the user avoids repetitive entries of user name and password pairs which may be seen as a barrier for rapid and simple access to resources. Depending on the actual implementation, single sign-on may blur the boundaries between service and authentication providers, and it may become unclear for the user who is providing a specific service and the privacy implications of using a service. This may challenge the data subject's information self-determination as the user may struggle in understanding the functioning of the system and the privacy implications of his or her own actions. However, providing the user with a lot of information regarding the processing of personal data may paradoxically be a burden for the user because it encourages or requires the user to stop and reflect on the relevance of the information. Consequently, there seems to be a more general tension between the goal of providing a seamless user experience and information requirements to ensure

98 See Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, pp. 150-156.

the principle of self-determination. If seamlessness leads to a non-transparent service, where the user does not know who can process his information and for what purposes, then it is questionable whether total seamlessness is at all desirable. From the perspective of data protection, a seamless integration of services should still ensure that the user can make informed decisions about how and by whom he or she wants personal data to be processed.

In the following we will analyse the Data Protection Directive's information requirements and the challenges these pose in identity management. In particular, we will address the difficulties of providing information, and how some of these difficulties may be overcome by introducing multi-layered short information notices (Section 4.1). Moreover, we will review the Liberty Alliance's specifications regarding technical mechanisms, i.e. XML-based privacy policies, to assist the user in making informed choices (Section 4.2).

4.1 Multi-layered information notices

The Data Protection Directive contains a number of provisions that oblige the controller to provide the data subject with information about the processing of personal data. The right to information is fundamental for ensuring that personal data is processed 'fairly and lawfully', as required by Article 6 (1) (a). Recital 38 explains that for the processing to be fair, 'the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection'. The Data Protection Directive contains also more specific information requirements regarding the information that should be made available before personal data is collected from the data subject (Article 10), information that should be provided when personal data have been obtained from third parties (Article 11) and information that should be offered before personal data are disclosed to third parties for the purposes of direct marketing (Article 14).[99]

The two most relevant provisions for the purposes of this paper are Articles 10 and 11, which distinguish between *essential information* that should be provided in all circumstances (identity of the data controller and of his representative, if any, and the purpose of the processing) and *further information* which should be provided if it is necessary to guarantee fair processing having regard to the specific circumstances in which the data are collected.

99 In addition, if personal data is processed on the basis of consent, the data subject must be provided sufficient information for the consent to be considered 'informed' in accordance with Articles 7 and 2 (h).

Regrettably, surveys show that compliance with and awareness of the current information requirements is a problem. In the Flash Eurobarometer 2003 company survey[100] only 37 % of the companies established in the EU Member States said they systematically provided data subjects with the identity of the controller, and only 46 % said they always informed data subjects of the purposes for which the data would be used. However, the problem is not only the companies' lacking compliance; a survey from 2003 revealed that only 42 % of EU citizens are aware that those collecting personal information are obliged to provide individuals with at least the identity and the purpose of the data collection.[101] Yet another problem is that on-line notices tend to be very long, using legal terms that are not easily understood by the average user. Such notices do not take into account that data collection usually happens rapidly and that extensive texts often do not fit well in a user-friendly interface. The added value for privacy and data protection of such long notices has therefore been questioned.[102]

There is no evidence suggesting that the situation regarding compliance with and awareness of data protection law is any better for identity management services. On the contrary, considering the complex organisational and technical aspects of many identity management schemes, there are reasons to believe that providing the data subject with relevant information is an important and challenging task. Identity management collaborations need an understandable way of communicating essential issues to their users. One possible solution for this challenge could be multi-layered information notices as suggested by the Article 29 Working Party.[103] This suggestion essentially allows

100 European Union companies' views about privacy (Flash Eurobarometer EB 147), 2003. http://ec.europa.eu/public_opinion/flash/fl147_data_protect.pdf.

101 European Union citizens' views about privacy (Special Eurobarometer 196), 2003. http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf

102 See e.g. the survey by Consumers International, 'Privacy@net, An International comparative study of consumer policy on the Internet', January 2001. http://www.consumersinternational.org/Shared_ASP_Files/UploadedFiles/80732215-7329-4A22-A02A-9A8062C65BC7_Doc30.pdf.

103 The Article 29 Working Party, 'Opinion on More Harmonised Information Provisions', 25 November 2004. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf. The proposal should be seen as an important step in a continuing development following from experience with the Data Protection Directive. The Article 29 Working Party's first contribution on this issue was the 2001 recommendation on minimum requirements for collecting personal data on-line. In its recommendation the Working Party gave concrete indications on how the Data Protection Directive should be applied to the most common processing tasks carried out via the Internet. The recommendation focused on when, how and which information must be provided, and was the first initiative to spell out on the European level a 'minimum' set of obligations for controllers operating web sites. Cf, Article 29 Working Party, 'Recommendation on minimum requirements for collecting personal data online', 17 May 2001. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf.

controllers to employ a simplified short notice in its user-interface, as long as the latter is integrated in a multi-layered information structure, where more detailed information is available. More specifically, the Working Party envisages that there could be up to three layers of information: (i) *the short notice*, which provides the essential information (and, in view of the circumstances, any additional information necessary to ensure fair processing); (ii) *the condensed notice*, which include all relevant information required under the Data Protection Directive; and (iii) *the full notice*, which include all national legal requirements and specificities. The notices should preferably be in a standardised table format which facilitates recognition and comparison between notices. Additionally, clear indication should be given as to how the individual can access additional information, e.g. by giving a link from one layer to another.

The rationale behind the multi-layered approach is that the quality of the information may be enhanced by focusing each layer on the information that the individual needs to understand in the current situation. Also, where space and time is limited, multi-layered formats can improve the readability of notices. With respect to the information that should be provided, the proposal follows the distinction in the Data Protection Directive between essential information that should be provided in all circumstances and further information which should be provided if it is necessary having regard to the specific circumstances in which the data are collected.

The Article 29 Working Party' proposal does not specifically address information requirements regarding identity management. However, this approach is highly relevant for providers of identity management services where information provisioning may be particularly challenging due to the involvement of numerous collaborators who integrate a variety of services and who may utilize personal information for diverse purposes.

The Article 29 Working Party's proposal for multi-layered information notices also seeks to address the lack of harmonization of information provision in Europe, which resulted from incorrect national implementation and from diverging interpretation and practice by supervisory authorities.[104] These differences led the Commission to conclude that '[t]he present patchwork of varying and overlapping requirements as regards information that controllers have to provide to data subjects is unnecessarily burdensome for economic

104 The European Commission, 'First report on the implementation of the Data Protection Directive', COM (2003) 265 final, p. 4. For example, some national laws stipulate that additional information must always be provided to the data subject, irrespective of the necessity test set out in articles 10 (c) and 11 (c).

operators without adding to the level of protection.'[105] This attempt to ensure 'a more harmonized interpretation of the Data Protection Directive's relevant provisions across the European Union'[106] can be contrasted with the Working Party emphasising that 'the sum total of the layers must meet specific national requirements, while each individual layer will be considered acceptable as long as the total remains compliant'.[107] Given the above mentioned national differences, it remains to be seen if the multi-layered approach succeeds as a basis for harmonized information provisioning.

Experience so far indicates that the principle of information self-determination is becoming more and more an illusion due to lacking compliance and awareness of the information requirements in the Data Protection Directive. Identity management represents new and sophisticated ways of facilitating and sharing data across organisations where provisioning of timely and relevant information in compliance with varying national implementations of the Data Protection Directive is a particular challenge. The Article 29 Working Party's proposal should therefore be of great interest for any provider of identity management services as it facilitates compliance and may also ensure the data subjects interests in understanding the privacy implications of using a particular service.

However, the potential in multi-layered notices depend on adoption by organisations and industry.[108] Hence, there is an important task for supervisory authorities to provide information on these notices and their benefits. The impact of multi-layered notices may also depend on how well they are implemented. For example, it is quite possible that subjects' awareness of privacy issues may be improved by standardised notices[109] which can easily be recognised and understood and which facilitate comparison between different services.[110]

105 Op.cit., p. 4. In order to ensure a more consistent approach to information requirements, the Commission included '[m]ore harmonised information provisions' as a specific action item of the work programme for a better implementation of the Data Protection Directive. Besides attempting to correct inconsistencies through dialogue with Member States and corrective legislative action, collaboration through the Article 29 Working Party was identified as an area of work.

106 The Article 29 Working Party, 'Opinion on More Harmonised Information Provisions', 25 November 2004, p. 6.

107 Op.cit., p. 7.

108 For example, Microsoft has shown interest in a multi-layered approach, see Fleischer, P. and Cooper, D., 'Microsoft's data privacy policies: EU Data privacy in practice – Microsoft's approach to compliance', Computer Law & Security Report 22, 2006, pp. 57-67.

109 Standardized notices are already being used by Creative Commons in the context of copyright, see http://creativecommons.org.

110 This question could be subject to an interesting empirical study.

4.2 Consent by way of machine-readable privacy policies?

Any processing of personal data is only lawful, if a number of legal requirements are fulfilled. In general, the processing of personal data may be lawful even without a contract or an explicit declaration of consent.[111] However, it is often useful to have the consent of the data subject, not least for the sake of clarity. Traditionally, such consent is received by e.g. obtaining a written declaration from the data subject, who consents to a particular processing of his or her data for specified purposes.[112] However, in a web-based interaction, which involves multiple controllers, it may be practically difficult and burdensome to obtain the data subject's consent in this manner. Therefore, we should also consider other ways to express consent. Such alternatives build on the idea that rights and obligations pursuant to personal data can be expressed in a rights management system, similar to digital rights management developed in the field of intellectual property law.[113]

The Liberty Web Services Framework supports mechanisms for rights management, allowing service providers and users to specify conditions for the

111 This is according to Article 7 (f) the case if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

112 For non-sensitive data, the Data Protection Directive requires 'unambiguous consent' in Article 7 (a). However, national data protection laws vary with respect to the formal requirements for declarations of consent. For example, in the UK, oral consent would be sufficient to fulfil the UK corresponding provision to Article 8(1) of the Data Protection Directive, see the UK Information Commissioner, Data Protection Act 1998: Legal Guidance, Version 1, 1998, paragraph 3.1.5. Germany, on the other hand, requires consent to be principally in written form, as stated in Bundesdatenschutzgesetz, Section 4 a (1) 3. Notably, 'in writing' also covers the electronic form according to BGB Section 126 (III). However, if consent is given in conjunction with other declarations, it needs to be clearly marked e.g. in bold. See, for further reference Gola, P. and Schomerus, R., Bundesdatenschutzgesetz, Kommentar, 8th edition 2005, pp. 167-168. With regard to the processing of sensitive data, the Data Protection Directive 95/46/EC principally refers to 'explicit consent' but there have been differences of opinion about what constitutes 'explicit consent'. For more analysis, see the PRIVIREAL project at http://www.privireal.org on consent and Kotschy, W. Commentary to Directive 95/46/EC, in Büllersbach, A. et al, Concise European IT Law, Alphen ann den Rijn, 2006, p. 47.

113 See e.g. Fahrmair, M., Sitou, W., Spanfelner, B., 'Security and privacy rights management for mobile and ubiquitous computing', http://www.ischool.berkeley.edu/~jensg/Ubicomp2005/papers/7-Fahrmair.pdf, last visited 26 January 2007.

use of data. Of special interest for this paper are *usage directives*,[114] which enable data subjects to communicate their privacy preferences, and services providers to communicate their privacy policy, with regard to the use of the data subject's personal data.[115] Hence, usage directives may be a means for service providers to comply with information requirements and for the user a means to set out restrictions for, or consent to, the processing of his personal data. However, their effectiveness may depend on how they are implemented by service providers and on the degree such mechanisms can be recognized by the law.

Liberty advocates a multi-levelled policy approach to usage directives, i.e. where a limited, hierarchical set of standardised privacy policies is used to describe the privacy practices of a service provider and the privacy preferences of the data subject. A simple example could be that the data subject first establishes a relation with a web services provider and declares a privacy preference for the release of his personal data by selecting one of the standard privacy policies. Later, when the data subject wants to perform a transaction with a service provider, this service provider will request attributes, e.g. name, address and billing information, from the web services provider holding the data subject's personal data. One of the standardised privacy policies accompanies the request and specifies how the service provider intends to use the requested information. If the privacy level of the service provider matches or is stricter than the data subject's privacy policy, the requested data is disclosed. If there is a conflict between the policies, the data subject may be notified about the conflict and be given the option of accepting or cancelling the transaction.[116]

The expressed rationale behind usage directives is to seek to automate the 'negotiation' of privacy policies between the parties. Machine-readable privacy policies in XML are already in use in current web browsers, based on

114 In the ID-WSF framework, participants may indicate the privacy policy associated with a message by adding one or more <UsageDirectice> header blocks to the SOAP header. See Liberty Alliance, 'Liberty architecture framework for supporting Privacy Preference Expression Languages (PPELs)', version 1.0 November 12, 2003, p. 4. http://www.projectliberty.org/liberty/content/download/371/2670/file/Final_PPEL_White_Paper.pdf

115 Liberty's usage directives allow for the use of any Privacy Preference Expression Language (PPEL). However, one of the most obvious candidates for expressing privacy policies is the Platform for Privacy Preferences (P3P). P3P 1.0 was launched as a W3C recommendation in 2002. It enables websites to express their privacy practices in a standard format, that can be retrieved automatically and interpreted easily by user agents. See further, http://www.w3.org/P3P/.

116 The Liberty Interaction Service allows a service provider to contact the data subject in real time when consent or permission is needed or when there is a mismatch between the privacy policies communicated by the data subject and the service provider. See, Liberty Alliance Project, 'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation', February 23 2005, p. 19.

the Platform for Privacy Preferences (P3P).[117] This platform enables an explicit expression of privacy practices for websites in a standard format. However, in contrast to the utilisation of P3P for exchanging privacy policies between a web browser and a website, usage directives facilitate a communication about the intended and allowed use of personal data between service providers. Typically, this will involve a service provider, who requests data regarding a user from another provider who holds this data. Hence, usage directives may be an important means to facilitate legitimate exchange of personal data between collaborating parties.

This process is sometimes discussed as 'automated privacy negotiation'.[118] However, data protection law, at least in Europe, does not use the concept of privacy negotiation. For the relation between the end-user and a services provider, any legally relevant communication would need to be classified in terms of contract or declaration of consent. The same would be the case for the 'negotiation' between two services providers about the exchange of personal information and the purposes these may be processed for. If we assume a situation in which the existing contracts do not justify the exchange of personal data, we are left with the issue of consent. We are then left with the following issues: 1) how can usage directives be used to consent, in a legally relevant way, to the processing of personal data? 2) If personal data, together with a usage directive, is disclosed by one controller to another controller, can this usage directive justify the latter controller's processing of personal data based on consent?

To our knowledge, these questions have only scarcely been addressed[119] so far, and depend on a number of factual elements which are still somewhat

117 See supra note 117.

118 See, e.g., Boyens, C., 'Privacy Trade-offs in web-based services', Berlin 2004, http://edoc.hu-berlin.de/dissertationen/boyens-claus-2004-12-15/PDF/Boyens.pdf, last visited 26 January 2007. For a legal analysis, see e.g. The Article 29 Working Party 'Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), June 1998. The Working Party has been critical to the use of P3P, stating that machine-readable policies must be applied within a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. See also EPIC 'Pretty Poor Privacy: An assessment of P3P and Internet Privacy', June 2000, which submits that the P3P specification builds on the weak 'notice and choice' privacy approach.

119 There is, however, a parallel discussion regarding the use of digital rights managements (DRM) systems, where protected content is made available, used, and eventually passed on by the end-user, see e.g. regarding a rights expression languages, Iannella, R. 'The Open Digital Rights Language: XML for Digital Rights Management', Information Security Technical Report, Volume 9, Issue 3, July-September 2004, Pages 47-55.

unclear.[120] However, with a few exceptions there are no explicit formal requirements to a declaration of consent under the Data Protection Directive, so an XML-based standardized notice would not be invalid for formal reasons, as long as the consent in natural language fulfils the material requirements.[121] Usage directives thus need to be understood together with textual data protection notices and other explanations. If the usage directive, understood in this context, contains relevant information about the processing (such as the purpose, if and to whom data will be communicated or how long it will be stored), it is difficult to see why these limitations should not be legally binding. The legal validity of a declaration of consent through a usage directive would, among other factors, depend on how the XML message is expressed in natural language for the end-user, whether this is understandable and not excessive, illegitimate or otherwise illegal under data protection law. Moreover, the experience with the use of P3P shows that due to the general low awareness regarding the possibilities of adjusting privacy preferences,[122] the default settings are of great significance. Consequently, great care should be taken in tailoring adequate privacy policies according to the service providers, business sector and type of data involved. Regard should not only be taken to applicable laws and regulations, it may also be advisable to involve e.g. data protection authorities to make sure that users' interests are taken into consideration. Based on the same considerations, it should be possible to consider a usage directive as a valid declaration of the user's consent communicated by one controller to another. Hence, if usage directives are to be used in an implementation of the Liberty specifications, the parties should make sure that their content fulfils the criteria for lawful processing and that the limitations expressed in the usage directives are made legally binding and enforceable.

However, a challenge with privacy preferences expressed in usage directives is that it is unclear whether service providers will actually comply with

120 See, e.g. Reidenberg, J. R. and Cranor, L., 'Can User Agents Accurately Represent Privacy Policies?', August 30, 2002. http://ssrn.com/abstract=328860, last visited 24 January 2007. Their conclusion is that the technological mediation designed to make it easier for users to understand the privacy practices of web sites risks adding ambiguity, confusion and legal uncertainty. In particular, 'the validity of automated actions or agreements between web sites and users for the use of personal information is jeopardized by inaccurate implementations', p. 13.

121 Some national data protection laws include formal requirements for declarations of consent. For example, according to the German 'Datenschutzgesetz', Section 4a (I), 3rd sentence, such declarations need to be in writing, save in exceptional circumstances. See further above, footnote 114.

122 See the Article 29 Working Party 'Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)', June 1998, p. 3.

the policy expressed in a privacy policy. The Liberty specifications contain no technical mechanism to ensure that the service provider's privacy policy is actually enforced. As long as there is no guarantee that the service provider will comply with the policy, the policy only reflects how the service provider intends to process the data. Users will probably only accept and rely on usage directives if they feel confident that the policies are respected and that the matching of policies verifiably follows the agreed logic.

5 Concluding remarks

There has been a swift development of identity management systems in the past, and there is no indication that history will stop here. On the contrary, we witness that truly integrated identity management systems are becoming implemented in a wider range of contexts. The arena has been dominated, and continues to be dominated, by information technology vendors and by schemes that are driven by the interest of the business and government, rather than end-users.

The uptake of federated identity management depends, however, also on the end-users trust in these systems in light of perceived and existing privacy risks. The early versions of multi-organisation identity management systems have taught us that inadequately designed systems may facilitate the generation of user profiles across organisational boundaries. This risk needs to be taken into account by anyone implementing such a system, and in particular by researchers developing the systems we will use in the future. Thus, the development of privacy-enhancing identity management systems should have continued priority in research and development.

Privacy and data protection are particularly challenging in a system where multiple parties collaborate. Hence, this paper has put considerable focus on the collaborative aspects of identity management, in which processes around authentication are delegated to third parties. This delegation will arguably increase in importance if the emerging notion of web services is put into practice. In the perspective of data protection law, this distribution of roles and responsibilities in authentication needs to be mapped to the available roles, i.e. controllers and processors. In practice this mapping is difficult, not only because the business processes are complicated, but also due to the generality of the available roles in data protection law and the lack of legal guidance about the collaboration between different actors. It may be the case that more targeted roles, like e.g. identity provider and web services provider in a new specific directive (similar to the E-Communications Directive) would solve some of these

issues. However, the aim of additional legislation should be simplification and enhanced clarity rather than additional bureaucratic burdens.

An additional challenge in identity management is the interaction with the end-user. There is a characteristic tension between, on the one hand, the desire to provide seamlessly integrated services and, on the other hand, the importance of providing the end-user with the understanding that is necessary to take informed decisions. This tension should result in a continued development of data protection law and practice, taking into account new possibilities like the above mentioned multi-layered approach to information provisioning. There should be a continued harmonisation in order to set down clear requirements that can be met by the involved actors and that actually lead to an increase in privacy protection – and not in bureaucracy and lengthy but worthless legal notes. The use of privacy policies and preferences may be important means to ensure compliance with information requirements and to ensure consent to the use and disclosure of personal data. However, their effectiveness may depend on how they are implemented, on user awareness and on their legal status.[123] Due to the low awareness about privacy and data protection issues, which has been documented in several surveys,[124] it is suggested that users should be able to choose between only a few and very easily understandable privacy preferences/policies. Also, circles of trust should preferably seek to agree on common privacy policies and to coordinate information provisioning in order to enhance transparency.

123 Notably, the legal status may also depend on the classification of the personal data to which the declaration of consent relates. As mentioned above in footnote 114, the Data Protection Directive requires explicit consent for the processing of sensitive data under Art. 8 (2)(a).

124 See e.g. surveys referred to in Section 4.1 (footnote 102, 103 and 104). More recent surveys in Norway also shows general low awareness of privacy and data protection issues among organisations and data subjects, see Ravlum, I., 'Processing of personal data in Norwegian organisations', TØI report 800/2005, http://www.toi.no/article18652-8.html, last visited 7 February 2007; Ravlum, I., 'Pinning our faith on Big Brother…togheter with all the little brothers', TØI report 789/2005, http://www.toi.no/attach/a1108468r559642/789_2005.pdf, last visited 7. February 2007.

KUNNSKAP SOM VERNET GODE – ET ESSAY*

Inger Marie Sunde

Kunnskap vs. Informasjon

Her skal noen rettslige sider av å anse kunnskap som et vernet gode presenteres. Det tas utgangspunkt i det klassiske kunnskapsbegrepet som avledes av menneskelig fornuft og fatteevne. Med andre ord: Uten mennesket ingen kunnskap!

Karakteristisk for vår tid er Maskinens store betydning for å behandle informasjon. Informasjon (og erfaring) er kunnskapens fundament, og på kort tid har datateknologien revolusjonert mulighetene for å produsere og utnytte informasjon. Utviklingen har bidratt til å befeste kunnskapens rolle i samfunnet i så stor grad at det nærmest er blitt en allmenn oppfatning at vi har gått inn i en epoke som trenger en ny merkelapp, nemlig «informasjons- eller kunnskapssamfunnet». «Nettverkssamfunnet» er ytterligere en betegnelse, nært knyttet til de to andre. Felles for uttrykkene er at de søker å få frem den store betydningen som informasjonsflyt har for økonomisk fremgang og samfunnsforholdene for øvrig. Uttrykkene anvendes til dels som substitutt for «globalisering» og kan tilsvarende kritiseres for å være akkurat like vage og intetsigende.

Ifølge den kjente sosiologen Manuel Castells kjennetegnes informasjonssamfunnet ved at informasjon har blitt et produkt i seg selv, og ikke bare er en innsatsfaktor i produksjon av andre ting.[1] Informasjonen flyter i globale nettverk. Castells fremhever hvordan moderne teknologi har opphevet avstand. Teknologien er i seg selv nettverk (tenk på moderne transportmidler og internett), som skaper og understøtter andre verdiskapende nettverk. I et nettverk behøver man ikke regne med avstand, fordi informasjonsflyten er så rask og kontakten så nær.[2]

---

* Inger Marie Sunde er stipendiat ved Det juridiske fakultet ved Universitetet i Oslo. Jeg takker for gjennomlesning og gode innspill fra professor Asbjørn Kjønstad og advokat Irina Eidsvold Tøien. Essayet er med mindre endringer tidligere publisert i *Kunnskapens vilkår – Akademikernes 10-årsjubileum*. Jon Bing (red.). 2007.

1 Manuel Castells The Information Age, Volume I, The Rise of the Network Society (2000) s. 78.

2 Castells karakteriserer utviklingsspranget som en overgang fra en kapitalistisk til en finansiell produksjonsmåte. Den finansielle produksjonsmåten er basert på kunnskap og informasjon, og understøttet av informasjonsteknologien. Ibid. s. 501-503.

Dette gir grunn til ettertanke. Det store tempoet i dagens informasjonsflyt har nok medført at vi er blitt vant til å tenke på nettverk som strukturer i samtid – for ikke å si sanntid («mens det skjer») – med internett som selve epitomet.[3] Men informasjonsflyt i nettverk er ikke i seg selv noe særegent for vår epoke. For eksempel kan den muntlige tradisjon, dvs. muntlige overleveringer mellom generasjoner, anses som informasjonsstrømmer i dynamiske nettverk hvor nodene kommer og går over tid.

For sterke generaliseringer kan dessuten bære galt av sted. Det nok være slik at avstand nærmest er opphevet for så vidt gjelder informasjonstilgangen. For et lite land som Norge, som i et historisk-geografisk perspektiv har ligget langt ute i periferien i forhold til universitetene på kontinentet (og verden for øvrig), innebærer derfor de teknologiske fremskritt en utjevnende effekt. Fremveksten av internett illustrerer dette; når enhver like lett kan anskaffe og spre informasjon, kan man ikke lenger snakke om informasjonssentrum eller -periferi.

Men det samme gjelder ikke for kunnskapsfrembringelsen. Kunnskap må man utvikle selv og da holder det ikke med klipp og lim av andres ideer. Kunnskap oppnås ved informasjonsforedling, refleksjon og overveielse. Dette krever tid. Selve kunnskapsprosessen er derfor neppe like kraftig påvirket av de teknologiske fremskritt som informasjonstilgangen. Utfordringen – som stadig gjelder – er; hvordan få kunnskapen til å blomstre? Dette er et spørsmål vi kommer tilbake til.

Hvordan vi benytter begrepene kunnskap og informasjon, er ikke helt likegyldig. Et menneske kan være informert. En datamaskin kan ikke ha kunnskap.[4] Datamaskinen utfører pr. definisjon automatiserte prosesser i henhold til instruks fra et menneske. Mange har erfart at datamaskinen tilsynelatende har begynt å leve sitt eget liv, og utført helt andre operasjoner enn man tror man har bedt den om. For eksempel tar den 32 000 utskrifter i stedet for én.

---

3 Man kan diskutere om internett bør skrives med liten eller stor forbokstav. Jeg synes man skal bruke liten forbokstav. Å insistere på å benytte stor forbokstav har ideologiske overtoner forankret i internetts opprinnelse for 30-40 år siden. Nå er internett blitt et allment utbredt nettverk; en tjeneste vi tar for gitt akkurat som telefonen. Å kreve at internett skal skrives med stor forbokstav kan sammenlignes med å kreve at vi må skrive Telefon eller Bil. Gisle Hannemyr argumenterer for Internett fordi nettet benytter TCP/IP-protokollen, se Hannemyr Hva er Internett (2005) s. 48. Det blir som å skrive Nordmann fordi vedkommende snakker norsk. Etter noe vakling har Norsk språkråd gått inn for stor forbokstav, jf. www.sprakradet.no. I praksis varieres det mellom stor og liten forbokstav.

4 Jeg går ikke inn på definisjonsproblemene som oppstår når man tilordner maskiner evne til å tenke, slik uttrykk som «kunstig intelligens» indikerer. Prinsipielt mener jeg at selv avanserte datasystemer neppe kan anses som mer enn hjelpemidler til å skape kunnskap hos mennesket. Men jeg mottar gjerne synspunkter på dette fra interesserte lesere. Sendes til i.m.sunde@jus.uio.no.

Men det er jo ikke maskinen som har vært ulydig; slike hendelser er som regel forårsaket av mennesker; kanskje skyldes det en alminnelig programmeringsfeil, eller kanskje en hackers forstyrrelser.[5]

Politikerne søker stadig via lovverket å styrke de forskjellige sidene av informasjonssamfunnet. Hvorvidt loven retter seg mot maskiner eller mennesker er ikke uvesentlig i så måte. Til tross for at verdiladete uttrykk som «human kapital» tyder på at kunnskap står høyt i kurs, retter mange politiske tiltak seg ensidig inn på å ivareta informasjon og er derfor nesten pr. definisjon tiltak for å sikre data og infrastruktur (såkalt informasjonssikkerhet).[6]

Her skal det ikke settes opp noe motsetningsforhold mellom kunnskap og informasjon, ei heller antydes at tiltak for å verne det ene skulle fungere til fortrengsel for det andre. Men man kan jo ikke utelukke at slike effekter kan forekomme, og uansett kan det være grunn til å dvele litt ved de ulike perspektiver som begrepene informasjon og kunnskap åpner for.

Noen betraktninger over det rettslige vernet

Informasjon som rettsobjekt

Man skulle kanskje tro at «informasjonssamfunnet» hadde sørget for å tilordne informasjon et vern på linje med det som gjelder for fysiske gjenstander, for eksempel slik at den som stjeler, underslår eller skader informasjon kunne straffes for det.[7] Loven yter imidlertid ikke et generelt strafferettslig vern om informasjon, noe det neppe er grunn til å stusse over. Det har sammenheng med det store avgrensningsproblemet som oppstår ved å anvende et informasjonsbegrep som verken er koblet til mediene eller stiller krav til informasjonens innhold.

Ifølge legalitetsprinsippet krever bruk av straff hjemmel i lov og straffebestemmelsen må være klar og presis.[8] Et ukvalifisert informasjonsbegrep ville

5 Utskriftseksemplet refererer seg til et skadeverk overfor datasystemene ved UiO sommeren 2007, hvor hackere hadde gjort endringer i programmene som styrer skriverne. For øvrig kan feilfunksjoner selvsagt også skyldes eksterne forhold som man ikke rår over, for eksempel strømbrudd som følge av lynnedslag. Også hardiskkrasj er en vanlig årsak til forstyrrelser.

6 Se f. eks. NOU 2006: 6 Når sikkerheten er viktigst. Forskning på IKT og IKTs betydning for forskning vies dog oppmerksomhet i St. meld. 17 (2006-2007) Eit informasjonssamfunn for alle kap. 5.

7 For den som vil se mer på dette, kan jeg vise til min bok Lov og rett i Cyberspace (2006) kap. 4, som inneholder en analyse av hvordan data vurderes i forhold til straffelovens gjenstandsbegrep.

8 Legalitetsprinsippet er nedfelt i Grunnloven § 96 «Ingen kan dømmes uden efter Lov».

neppe oppfylt et slikt kriterium. Informasjon strømmer jo fra et utall medier som for eksempel kringkasting, bøker, musikkspillere, personer (i ord og handling), datasystemer og kulturelle markører.[9] Formidlingen varierer med mediene og dessuten er innholdet i det som formidles svært forskjellig. Det er jo stor forskjell på en personlig betroelse og en TV-sending, men begge deler er informasjon. Og kanskje er det så stor forskjell mellom betroelser også, at de bør behandles forskjellig. Bør for eksempel en betroelse overfor prest eller lege, være rettslig likestilt med private betroelser mellom venner? Lovgiver synes det bør være en forskjell, og har oppstilt en straffesanksjonert taushetsplikt for betroelser i profesjonsforhold, mens rent private betroelser er prisgitt lojalitetens styrke.[10] Et unntak gjelder dog vitneplikten som innrømmer et visst vern for fortrolighet i familien. Man er således fritatt for å vitne om forhold som gjelder et familiemedlem som er siktet i en straffesak.[11] I sivil saker gjelder en lignende regel.[12]

Iblant kan man dessuten lure på om det i det hele tatt er informasjon som formidles, som for eksempel når en person snakker «nytale» eller «kaudervelsk».[13] Det vil igjen avhenge av om informasjonsbegrepet kobles til vilkår om å være sant eller forståelig. Disse eksemplene illustrerer noen av problemene lovgiver står overfor når det er tale om å bygge opp et lovfestet vern om informasjon.

Indirekte gir imidlertid loven et vern, ved at den kriminaliserer bestemte måter å skaffe seg informasjon på. Det er for eksempel straffbart å skaffe seg informasjon ved brevbrudd, innbrudd på en datamaskin eller ved avlytting.[14] Det spiller ingen rolle for straffbarheten om innholdet er hemmelig eller av spesiell karakter for øvrig. Dessuten foreligger det en rekke rettslige insentiver til å formidle informasjon som er sann, blant annet ved at loven slår ned på bedragerivirksomhet og falskneri, regnskapsjuks, bevisst feilinformasjon til ak-

9 Se noen refleksjoner rundt bruken av begrepene informasjons- og datasikkerhet i Lov og rett i Cyberspace op.cit. s. 30-31.

10 Straffeloven § 144 setter straff for å åpenbare hemmeligheter som er noen betrodd i bestemte profesjonsforhold.

11 Straffeprosessloven § 122.

12 Tvistemålsloven § 207.

13 Nytale er myndighetenes språk i George Orwells 1984. «Kaudervelsk» kommer fra tysk som en betegnelse på det språket italienske og franske kjøpmenn brukte i Sør-Tyskland. Uttrykket er avledet av kaudern: kramhandel og welsch ('velsk'): uforståelig språk. Ref. Bokmålsordboka. www.sprakradet.no. Man kan jo spørre hvordan kaudervelsk er blitt betegnelsen på noe uforståelig når kjøpmennene utvilsomt forsto det. Den sannsynlige akademiske forklaring er at utenfraperspektivet trumfet innenfraperspektivet. En annen, men identisk formulering, er at de som ikke forsto kaudervelsk følte seg ekskludert og kalte det uforståelig. Deres begrepsbruk vant frem.

14 Straffeloven §§ 145 første og annet ledd og 145a.

sjemarkedet, i markedsføringen av varer og tjenester osv. Selve velferdsstaten er tuftet på et tillitsbasert system hvor fordelingen av trygde- og sosialytelser, skatter og avgifter, beregnes etter opplysninger gitt av borgeren. Siden staten har begrensede ressurser til å drive kontrollvirksomhet, og det dessuten sikkert går en grense for hvor omfattende kontroll som er ønskelig, er systemet avhengig av at opplysningene som inngår i beregningsgrunnlaget, er fullstendige og korrekte. Derfor reageres det strengt på feilinformasjon. Grunnleggende sett handler det om et tillitsbrudd overfor fellesskapet.

Hemmeligheter

Via en del spesialregler gir loven vern for informasjon av kvalifisert art. Regler for behandling av personopplysninger er et praktisk eksempel, men om dette temaet er det allerede skrevet så mye at jeg lar det ligge her.

En klasse for seg er stats- og bedriftshemmeligheter, som det er straffbart å anskaffe, røpe og benytte.[15] Personlige hemmeligheter derimot, har ikke noe generelt vern, men å gjøre dem kjent kan etter omstendighetene være straffbart som æres- eller fredskrenkelse (privatlivets fred).[16]

Begrepet «hemmelig» er ikke helt enkelt, og et spørsmål er hvordan man skal vurdere bruk av «åpne kilder». Spørsmålet har fått økt betydning ved utbredelsen av internett, som gir en historisk sett unik tilgang til forskjellige informasjonskilder. Kan det som er åpent være hemmelig?

Puslespilldoktrinen

I den såkalte Loran C-saken fra 1982 ble to fredsforskere dømt for rettsstridig besittelse og åpenbaring av statshemmeligheter.[17] Saken peker seg ut som interessant også nå 25 år senere, fordi hemmelighetene som lå til grunn for domfellelsen nettopp besto av opplysninger de hadde sanket inn fra åpne kilder. Høyesterett sa at spørsmålet gjaldt om opplysningene på forhånd var så lite kjent at de kunne betraktes som hemmelige i lovens forstand, og anla en helhetsvurdering for å ta stilling til dette. Opplysningene var bearbeidet og fremlagt i en forskningsrapport som dannet et omfattende systematisert materiale og ga et detaljert bilde av bestemte forsvarsinstallasjoner. Det ble lagt til grunn at materialet hadde stor militær verdi for en potensiell angriper. Høyesterett konkluderte med at materialet var å anse som hemmelig i straffelovens forstand. Dermed var

15 Straffeloven §§ 90, 91, 294 nr. 2 og 3 og 405a. Markedsføringsloven § 7, jf. § 17.
16 Straffeloven §§ 246, 247 og 390.
17 Rt. 1982 s. 426. Saken omtales også som Gleditsch/Wilkes-saken etter navnene til fredsforskerne. De ble domfelt for overtredelse av straffeloven §§ 90 og 91.

den såkalte «puslespilldoktrinen» etablert; det er merverdien i den systematiske informasjonsinnsamlingen og analysen som representerer hemmeligheten.

Med den sikkerhetspolitiske betydning forskningsrapporten den gang hadde, kan man forstå resultatet i Loran C-saken. Men hvis man tenker på dagens store mulighet for enkel og effektiv utnyttelse av åpne informasjonskilder, representerer Høyesteretts resonnement et tankekors. Hvor mange opplysninger har man lov å sammenstille og hvordan kan analysen utføres og presenteres? I det uryddige sikkerhetspolitiske landskapet som hersker i dag, er det ikke nødvendigvis lett å manøvrere verken for forskere eller journalister som vil bidra til folkeopplysningen i demokratiet.

Man kan spørre om puslespilldoktrinen også gjelder for «informasjonsmegling» i det private markedet. Såkalte informasjonsmeglere avdekker strategisk informasjon om kommersielle aktører, og selger informasjonen til konkurrentene. Det hersker nok en utbredt oppfatning om at så lenge man samler inn informasjon fra åpne kilder er man på trygg grunn, men det er jo bare holdbart hvis puslespilldoktrinen ikke kommer til anvendelse. Og det er neppe utelukket at både informasjonshøstingen og analysen etter omstendighetene kan anses som urimelig anskaffelse av bedriftshemmeligheter, dersom virksomheten blir for nærgående. Slik virksomhet kan dermed komme til å befinne seg i en juridisk gråsone i forhold til straffelovens bestemmelser.[18]

Lundutvalget har kritisert puslespilldoktrinen og fremholdt at «innsamling og analyse av informasjon fra åpne kilder med sikte på å avdekke hva som foregår i samfunnet, i utgangspunktet både er legitimt og ønskelig». Slik aktivitet bør derfor kunne skje uten risiko for strafforfølgning. På den annen side fremholdes det at avsløring av det som blir helhetsresultatet neppe bør kunne skje straffritt, når det utgjør en hemmelighet av betydning for rikets sikkerhet. Utvalget tar til orde for en nyansering av reglene i forhold til dagens bestemmelser, for å sikre den frie adgangen til informasjonssanking.[19]

Iblant utsetter informasjonsteknologien oss for nye prøvelser, noe den såkalte Kværner-saken er egnet til å illustrere.[20] Saken gjaldt feilsending av epost som følge av at to menn i 30-årene hadde registrert domenet Kvearner.com. Ikke overraskende ledet det til forveksling med domenet Kvaerner.com som var registrert av selskapet Kværner ASA. Siden bokstaven «æ» ikke er tilgjengelig i domene-språket, hadde registrantene skaffet seg domenene i henhold

18 I arbeidet med ny straffelov har Straffelovkommisjonen forslått at reglene om rettsstridig anskaffelse og utnyttelse av bedriftshemmeligheter overføres til en ny regel om brudd på bedriftshemmelighet. Informasjonsmegling er ikke omtalt. NOU 2002: 4 Ny straffelov s. 323.

19 NOU 2003: 18 Rikets sikkerhet s. 70, 73 flg. og 156.

20 Rt. 2003 s. 825.

til hvert sitt syn på hva som var den naturlige representasjonen av «æ». De tiltalte hadde anvendt tegnkombinasjonen «ea» som reflekterte den engelske uttalen av Kværner (som i verbet «to earn»), mens Kværner hadde valgt den norske formen, nemlig «ae». En konsulent som hadde i oppdrag å utarbeide en hemmelig strategi for Kværner, med sikte på å hindre Aker Engineerings oppkjøp av selskapet, la strategidokumentet som vedlegg til en epost til Kværner som han hadde skrevet på engelsk. Og han tenkte vel også på engelsk da han skrev epostadressen. Eposten og vedlegget havnet følgelig hos de som senere ble tiltalt. Tiltalen var basert på at de hadde skaffet seg en bedriftshemmelighet på urimelig måte, fordi de hadde åpnet vedlegget til tross for at de skjønte at eposten var feilsendt og at vedlegget inneholdt en bedriftshemmelighet. Dette fremgikk jo med all tydelighet av eposten som var merket «final board presentation» og «strictly confidential». Oppkjøpsstriden var dessuten velkjent for de impliserte. Høyesterett uttalte at loven ikke rammer den som kommer i besittelse av en bedriftshemmelighet ved en tilfeldighet, men mente anskaffelsen i dette tilfellet var å anse som urimelig og straffbar.

Vi kan merke oss avgjørelsens beskrivelse av bedriftshemmeligheten; det var et dokument som «bygde på offentlig tilgjengelig materiale m.h.t. regnskapstall m.v., men inneholdt vurderinger og forslag til forskjellige strategier mot oppkjøpet. Etter Kværners mening ville det være svært uheldig om dette dokumentet kom på avveier.» Som i Loran C-saken bygde innholdet på informasjon fra åpne kilder, det sentrale var bearbeidelsen og analysen. Informasjonsforedlingen og konsulentens anbefalinger ga dokumentet verdien, en verdi som avhang av at det ble holdt hemmelig til kritiske faser i oppkjøpsstriden var passert. Både analysen og den subjektive oppfatning til den som ble rammet av eksponering ble altså tillagt betydning. Dette er i tråd med rettsoppfatningen i Loran C-saken.

Passord

Vi går nå over til en annen type hemmelighet som har stor funksjonell utbredelse i informasjonssamfunnet, nemlig passord og andre koder. Vern om slike koder er et tema som volder rettslig hodebry i mange sammenhenger. At koder bør ha et rettslig vern er neppe kontroversielt i seg selv. En kode som er blitt kjent mister jo sin verdi og noen aktverdige grunner til å eksponere dem synes det vanskelig å få øye på. Uberettiget eksponering kan sammenlignes med å spre kopier av en vanlig husnøkkel.

Det er sikker rett at en kode kan anses som utbytte av en straffbar handling. Dermed kan man dømmes for såkalt informasjonsheleri dersom man, for

eksempel, mottar en kode man mener er avdekket ved en kriminell handling.[21] Denne rettsoppfatningen ble lagt til grunn av Høyesterett allerede i 1995.[22] At det kan være praktisk behov for å slå ned på tilfeller som gjelder passord på avveie, illustreres i en dom fra 2003.[23] Saken gjaldt heleri av 650 000 passord som ga adgang til epostkonti administrert av en norsk eposttilbyder.

I 2005 ble det inntatt en ny bestemmelse i straffeloven som uttrykkelig gjør det straffbart å spre passord som gir tilgang til et datasystem.[24] Man kan spørre hva bestemmelsen mener med «datasystem». At datamaskiner av den typen vi har hjemme og på kontoret, omfattes, er sikkert nok. Men omfattes også alle andre typer tilgangskontrollerte maskiner med automatiserte prosesser, og hva med tilgangskontrollerte tjenester som man kan disponere via en datamaskin? I så fall verner bestemmelsen for eksempel også pin- og andre sikkerhetskoder til bankkort m.v., som kan anvendes ved bruk på minibank, automatiserte bensinpumper og transaksjoner på internett. Om dette tier lovbestemmelsen og spørsmålet er ikke kommentert under lovforberedelsen.[25]

Passordmisbruket som sådan har ikke noen selvstendig rettslig relevans etter dagens regler, dog med forbehold for de rene databedragerier. Kjøp av tjenester på internett ved bruk av stjålet bankkort skal visstnok anses som databedrageri, jf. straffeloven § 270 nr. 2. I den «fysiske» verden legges det størst vekt på arten av det godet man har skaffet seg adgang til. Er det tale om uberettiget adgang til data, skal en spesialregel i straffeloven § 145 anvendes, mens uberettiget uttak fra minibank og bensinpumper er å anse som tyveri, jf. straffeloven § 257.[26] Lik fremgangsmåte (avgivelse av kode) kan altså gi forskjellig rettslig bedømmelse. Det viktigste er antakelig å huske at det uansett er straffbart å misbruke koden. Straffebestemmelsene får juristene holde styr på.

Et annet spørsmål er hvem som «eier» en kode.[27] Spørsmålet er ikke direkte lovregulert, og som et generelt utgangspunkt må man nok nøye seg med å si at svaret varierer med grunnlaget for at man disponerer koden. Dersom koden refererer seg til en personlig bankkonto, kan nok innehaveren disponere den

21 Hvis dette er noe man tror, men som ikke lar seg bevise, skal man bare dømmes for forsøk på informasjonsheleri.
22 Rt. 1995 s. 1872.
23 Nedre Romerike tingretts dom 25. november 2003.
24 Straffeloven § 145b.
25 NOU 2003: 27 Lovtiltak mot datakriminalitet (I), s. 21 flg. Ot.prp. nr. 40 (2004-2005) s. 20 og 33.
26 Rt. 1997 s. 1771. Se også Lov og rett i Cyberspace op. cit. s. 189-191.
27 «Eier» settes i anførselstegn siden slike koder er informasjon som ikke eies i vanlig betydning av ordet. I Sverige har man utredet om lovverket bør etablere eiendomsrett til informasjon, og konkludert negativt. SOU 1992: 110 Information och den nya Informationsteknologin s. 155-157.

som hun vil, men da slik at hun også har tapsrisikoen ved eventuelt misbruk som følge av at koden har vært oppbevart på uforsvarlig måte. Spørsmålet om hva som er aktsom oppbevaring av koden, har vært oppe til behandling for domstolene ved et par anledninger.[28] I et tilfelle er det lagt til grunn at å kamuflere pinkoden som et telefonnummer ikke er forsvarlig, mens det har vært godtatt at koden er nedskrevet i en «7. sans» som ligger i en låst koffert i en låst leilighet.[29] Uforsvarlig oppbevaring gjør uansett ikke tredjemanns bruk av koden rettmessig; dét krever særskilt samtykke eller fullmakt. Uttakene er således å anse som en straffbar handling. At den lovlydige borger er i en skvis mellom sikkerhetskrav og praktiske forbrukerbehov, er imidlertid klart. Dette kalles «passordtyranniet».

Et praktisk forhold som ikke har vært særlig påaktet før i et utredningsarbeid utført av Datakrimutvalget i 2007, er hvilke forpliktelser som knytter seg til koder man disponerer i kraft av sitt arbeidsforhold, typisk det personlige passordet til arbeidsplassens datasystem. Hva hvis man «låner» det bort til en annen som ikke har noen selvstendig rett til å benytte systemet? Kan det anses som medvirkning til uberettiget tilgang til datasystemet, eller er handlingen rettmessig fordi arbeidstakeren kan disponere sitt område som hun vil?

På det generelle plan fremholder Datakrimutvalget bedriftens behov for vern om datasystemet, og at personlige brukerrettigheter normalt gis i en relasjon basert på tillit og lojalitet. Utgangspunktet er derfor at arbeidstakeren anses å besitte passordet på vegne av bedriften og ikke rettmessig kan gi det videre uten særskilt tillatelse.[30]

Utvalget har for øvrig foreslått en egen straffebestemmelse som rammer enhver rettsstridig befatning med passord og andre såkalte tilgangskoder. Bestemmelsen vil, dersom den blir vedtatt, gi et langt mer omfattende vern for koder enn det som følger av dagens regler. Et praktisk tilfelle som i så fall kan bli klart straffbart, er «passordknekking». Hvorvidt dette er straffbart i dag, for eksempel fordi det anses som uberettiget adgang til data, er usikkert.[31] Passordknekking betyr å gjette data, personlig eller maskinelt. Den maskinelle passordknekking som skjer ved «ordbokangrep» eller «rå kraft» er det liten grunn til å forsvare. Men den intuitive gjetting, for eksempel av kollegaens passord som er navnet til kjæledyret, er vanskeligere å klandre. Her kan den interesserte leser slå opp i Datakrimutvalgets betraktninger, eller avvente

28 Dessuten foreligger en mer omfattende praksis fra Bankklagenemnda.
29 RG 2002 s. 1273, Rt. 2004 s. 499.
30 NOU 2007: 2 Lovtiltak mot datakriminalitet (II) s. 64 flg.
31 Hjemmelen er i så fall straffeloven § 145 annet ledd.

Regjeringens forslag til datakrimbestemmelser i den nye straffeloven som er under utarbeidelse.[32]

Listen over kontroversielle informasjonsspørsmål kan gjøres lang og hvert av dem er gjerne så komplisert at det fortjener en avhandling alene. Her skal jeg bare kort skissere to aktuelle problemstillinger som er blitt såkalte «juridiske minefelt». Det ene knytter seg til åpen kildekode, det andre til mellommannsansvaret på internett.

Kildekode og Kerckhoffs' prinsipp

Kildekode er den menneskelig forståelige oppskriften til et dataprogram. At kildekoden er «åpen» betyr at den frigis til omverdenen. Dersom programvareprodusenten velger å beholde kildekoden som en bedriftshemmelighet, sier man at den er «lukket». Det gjøres for eksempel av strategiske grunner, slik at konkurrenter ikke skal få innsyn i og kunne utnytte teknologien som ligger til grunn for dataprogrammene. Kildekoden representerer imidlertid et verdifullt informasjonstilfang for samfunnet; dersom man kan bygge videre på andres ideer går jo utviklingen mye raskere enn om man skal finne opp hjulet på nytt hver gang. Et godt eksempel på hvor verdifull åpen kildekode kan være, er internetteknologien med sitt vell av tjenester, som er resultatet av innsats fra utviklere over hele verden som har delt og utnyttet åpen kildekode.[33]

Av slike grunner gir loven rett til å undersøke et dataprogram for å avdekke de ideer og prinsipper som ligger til grunn for de forskjellige delene av programmet. Videre kan man foreta såkalt omvendt utvikling, som er forsøk på å reversere objektkoden til kildekode.[34] Her tillegger altså loven samfunnets og forskningens behov større vekt enn produsentenes strategiske interesser. Man kan også si at loven på dette punkt prioriterer kunnskapsutvikling fremfor mer rendyrkede kommersielle interesser.

Men hva hvis legitim analyse resulterer i at man avdekker koder som er lagt inn i programvaren, av mangel på bedre steder å legge dem? Slik teknologi har vært anvendt på DVD-spillere for å beskytte mot filmpirateri, og var kjernen i den såkalte DVD-saken.[35] Skal koden i et slikt tilfelle anses å være i allment eie, eller skal man også her prøve å opprettholde et rettslig vern for koder? Datakrimutvalget har forsøkt å løse dette spørsmålet også, og foreslått at det ikke gjøres straffbart å komme over koder som ledd i lovlig analyse, mens den

32 Op.cit. s. 158.
33 Gisle Hannemyr har skrevet engasjert om dette i Hva er Internett op. cit. s. 130 flg.
34 Åndsverkloven §§ 39h og 39i.
35 RG 2004 s. 414.

fortsatte besittelse eller spredning av slike koder foreslås gjort straffbar. I den forbindelse vises det til Kerckhoffs' prinsipp, en gammel kryptologisk maksime som sier at sikkerheten ikke skal hvile på at algoritmen (les kildekoden) holdes hemmelig, bare på at koden er hemmelig. Algoritmen bør alle kunne studere. Mannen bak prinsippet, Auguste Kerckhoffs (1835–1903), virket forresten som professor i lingvistikk i Paris og publiserte sitt berømte prinsipp i essayet La Chryptographie Militaire i 1883.[36]

Åpen kildekode er ofte lisensiert under den såkalte GPL-lisensen, som i sin tid ble etablert av den kjente utvikleren Richard Stallmann.[37] Den sentrale lisensbetingelsen er at man må avstå fra å lukke kode som er utviklet på grunnlag av GPL-lisensiert kode. Dermed sikres fortsatt innsikt i teknologien for informasjonsallmenningen. Også rekkevidden av forpliktelsene i denne lisensen gir opphav til en mengde interessante spørsmål for jurister.

Mellommannsansvaret; nettverter og tekniske filtre

For så vidt gjelder mellommannsansvaret på internett byr det seg her en anledning til å peke på et stort tankekors: Ifølge ehandelsloven kan ikke en «nettvert» holdes ansvarlig for tjenestemottakerens ulovlige virksomhet, for eksempel i form av spredning av datavirus eller overgrepsbilder av barn. Unntak gjelder dersom nettverten var klar over den ulovlige virksomheten, dvs. hadde «forsett». Da kan det strafferettslige medvirkningsansvaret anvendes.[38] Lovens formål er å sikre fri flyt av informasjonsbaserte tjenester, og likelydende regelverk gjelder i hele EU/EØS-området. Mellommenn er nødvendige aktører i informasjonsformidlingen, men representerer en kontrollerbar flaskehals og er derfor et potensielt hinder i denne flyten.

Tankekorset er at loven er skrevet som om «nettverten» var en fysisk person, mens det i realiteten er tale om en lagringstjeneste som tilbys av foretak som normalt er ganske store (for eksempel Telenor), og som rent konkret utføres av datamaskiner, såkalte vertsmaskiner (eng: «host»). En maskin kan ikke være klar over noe som helst og kan følgelig ikke ha «forsett». Regelverket har på denne måten positivt utelukket muligheten for å oppfylle det som er et grunnvilkår for ansvar, nemlig kunnskap om hva man foretar seg, og risikoen

36 Han var døpt med det klingende navn Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof. Han syntes vel navnet var litt tungtvint og forkortet det til Auguste Kerckhoffs.

37 Lisensens fullstendige betegnelse er GNU General Public License. Den kalles også «copyleft» som kontrast til de tradisjonelle reglene om «copyright».

38 Ehandelsloven § 18 bokstav a. Tjenestemottaker er for øvrig ehandelslovens uttrykk for abonnent eller kunde.

for straff er dermed effektivt eliminert. I praksis finnes det derfor ikke risiko for mellommannsansvar for nettverter.

Da skulle man til gjengjeld tro at man kunne anvende tekniske filtre for å hindre gjennomstrømming av illegalt materiale. I praksis filtreres det jo mot datavirus, så hvorfor ikke mot overgrepsbilder også? Men nei, samme lov presiserer at nettverten ikke har plikt til noen «generell» overvåking, eller til å undersøke forhold som antyder ulovlig virksomhet.[39] Dermed elimineres plikt til å bruke moderne utstyr som kan filtrere for illegalt materiale. Eller kanskje ikke? Kanskje vi kan anse filtrering for en bestemt type illegalt materiale som «spesiell» overvåking, som ikke omfattes av forbudet? Og kanskje filtrering ikke anses som overvåking i det hele tatt, slik at det er forenlig med loven allerede av den grunn? Denne usikkerheten om hva regelverket egentlig innebærer er med på å redusere handlekraften overfor alvorlig kriminalitet.

Innføringen av dette regelverket illustrerer en betenkelig side ved den internasjonale regelproduksjonen, hvor man for å fremme økonomiske sektorspesifikke behov, nærmest med et pennestrøk eliminerer sentrale ansvarsregler som har lang tradisjon i det nasjonale rettssystemet.

Vern om kunnskap

Det er neppe behov for å gjennomføre en stringent rettslig sondring mellom informasjon og kunnskap i hele lovverket. Som vi har sett finnes andre begreper som er bedre egnet til å få frem poenget i de forskjellige rettssetningene, slik som «hemmelighet» som omfatter begge deler. Dette skaper ikke noe problem.

Det er heller ikke gitt at et valg mellom rettstradisjoner som setter henholdsvis den menneskelige eller maskinelle produksjonsevne i sentrum, nødvendigvis har stor betydning. Vi er for eksempel vant til å tenke på opphavsretten som et viktig insitament for menneskelig skaperkraft. I den kontinentaleuropeiske opphavsrettsdoktrin som norsk rett er utslag av, anses opphavsretten å oppstå som en personlig rett i kraft av åndsverket. Doktrinen betegnes da også som «author's right» eller «droit d'auteur» (den har sitt opphav i begivenheter på 1500-tallet i Frankrike). I anglo-amerikansk «copyright»-doktrin er imidlertid retten til å produsere eksemplarer av verket det sentrale, og denne rettigheten ble opprinnelig tildelt som en form for kongelig privilegium til boktrykkerne. Forfatteren hadde ikke noen personlig rett til innholdet i sitt manus som sådan.[40] Den ene doktrinen setter det kreative mennesket i sentrum, den andre gir rettigheter til eieren av en god maskin. Men likevel, begge rettstradisjoner

39 Ehandelsloven § 19.
40 Hans Marius Graasvold, Eirik Djønne og Jon Bing Norsk skribentrett (2006) s. 15-18.

synes å ha fungert tålelig bra til tross for den fundamentale forskjellen i opprinnelse og begge strever med utfordringene fra den digitale teknologien.

På det allmenne plan kan vi slå fast at markedsideologiens frie flyt er nedfelt i lovverket, mens flere aktuelle problemstillinger etterlater spørsmål om vi har funnet den rette balansen mellom markedsmessige behov, og enkeltindividers og informasjonsallmenningens behov. Bare tenk på hvordan man behendig har unnlatt å overføre det anerkjente redaktøransvaret til debatt formidlet på nett. Som om det er noen grunn til å behandle debatt på nett annerledes enn den som foregår i avisen eller i en direktesending på TV!

Som middel til å sikre forskningens kår har lover likevel begrenset betydning. Faktisk informasjonstilfang og mulighet for refleksjon og overveielse er nok langt viktigere. Informasjonssamfunnets eliminering av tid kan derfor være et problem for kunnskapsproduksjonen. Hva blir produktet; kunnskap og erkjennelse eller overflatebetraktninger og forvirring?

Holbergs anstrengelser for å delta i det kontinentale forskernettverket på 1700-tallet gir noen interessante perspektiver i så måte. Visstnok var Ludvig Holberg (1684–1754) vår første ordentlige vitenskapsmann og den «fremste reformator» av det dansk-norske åndsliv i sin tid. Sine berømte komedier skrev han i løpet av en 10-års periode som han kalte sin «poetiske raptus», midt i et langt liv dedikert til vitenskapen.[41] Man kan ikke annet enn beundre Holbergs vitebegjærlighet. Med sitt statsstipend på 100 riksdaler i året, vandret han på sine nette føtter til Paris og Roma, for å studere skriftsamlingene der – og hele veien hjem igjen – bare hjulpet av et par båtstrekninger. Økonomien tillot ham ellers ikke å kjøpe seg transport. Men som det er skrevet; «føttene var gode og han forsto kunsten å gå».[42] Hva man ellers kan si om studieforholdene, den bokstavelig talt *medgåtte* tid ga i hvert fall gode muligheter for refleksjon og overveielse!

Tilfellet Holberg sammenholdt med kjennetegnene ved dagens informasjonssamfunn gir således grunnlag for følgende gåte: Hvis lav informasjonstilgang og god tid gir høy kunnskap, hva er så produktet av høy informasjonstilgang og lite tid? Løsningen overlates det til den oppvakte leser å utlede.

41 Torleiv Kronen Ut over grensene (1985) s. 34-47.
42 Ibid. s. 39.

KNOWLEDGE ECONOMY THEORIES UNDERPINNING EU'S I2010 STRATEGY AND THEIR (IN) CAPACITY FOR REPRESENTATION IN A REGULATORY FRAMEWORK FOR NIGERIA*

Peter Chukwuma Obutte

Part 1

Introduction

The emerging trends of technological revolution and convergence in communications services, networks, and their regulation, have since necessitated the need for nation-states to re-examine their preparedness for these realities. It has also encouraged regional alliances to confront the likely socio-economic impacts.

In summing this reality, Manuel Castells notes that:

> *«…digital networks are global, as they know no boundaries in their capacity to reconfigure themselves. So, a social structure whose infrastructure is based on digital networks is by definition global. Thus, the network society is a global society. However, this does not mean that people everywhere are included in these networks. In fact, for the time being, most are not. But everybody is affected by the processes that take place in the global networks of this dominant social structure.»*[1]

In that connection, the paper proceeds from basic theoretical commentaries on knowledge economy and the underlying significance it presents for the European Union and the EUi2010 initiative. The paper examines empirical considerations and comparative elements to determine the possibility of representing the EUi2010 initiative in the Nigerian context, to meet its needs.

---

* This represents my 'prescribed' trial lecture for the Dr.Juris degree presented on September 27, 2007.

1 Manuel Castells (2004 a), The Network Society: A Cross-cultural Perspective', Edward Elgar Uk, page 22.

In this paper, I will contend that the application of an initiative similar to EUi2010 in Nigeria will be a misplaced priority at this phase of the country's development.

To discuss the issues, the paper is divided into two parts.

The focus of Part 1 is on Europe; as it will briefly discuss theories about knowledge economy and EUi2010, the European Information Society 2010 and its significance. The scope of part two will be about Nigerian's needs, and followed by a few concluding remarks.

Theories of Knowledge Economy & EUi2010

The theories of knowledge economy that underpin the EUi2010 could provide a wide variety of explanations and options in responding to the evolving benefits and challenges of information society as they relate to traditional system of quality of people's livings conditions.

The Knowledge Economy is considered as an extension of the Information Society in which the creation, distribution, diffusion, uses, and manipulation of information is a significant economic, political, and cultural activity.[2] Knowledge Economy and Information Society have both come to be identified as successors to industrial society; and have been described with concepts such as post-industrial society (propounded by Daniel Bell), post-modern society, informational capitalism, network capitalism, knowledge society, and the network society (advanced by Manuel Castells).[3]

The emerging relationship between productivity, competitiveness and the welfare state is exemplified by a study on the Finnish knowledge economy model. It traces sustainable growth to investing in home-grown, human capital, and improving standards of living that strengthen the social sources of productivity in the new, knowledge-based economy.[4]

However, challenges do exist; as pointed out in the commentary that 'the instrumental capacity of the nation-state is decisively undermined by the globalization of core economic activities, by the globalization of media and electronic communication, by the globalization of crime, by the globalisation of social protest, and by the globalization of insurgency in the form of transborder terrorism.'[5]

---

2 'Information society' at: http://en.wikipedia.org/wiki/Information_society, accessed on September 14, 2007.

3 See footnote 2, supra.

4 Castells, Manuel (2004 b), 'The Information Age: Economy, Society, and Culture' Blackwell Publishing, Oxford, page 315

5 Castells, Manuel (2004 b), page 304

There was a need therefore, to resolve the contradictions of operating in globalized and integrated markets while experiencing major cost differentials in social benefits as well as distinct levels of regulation between countries.[6]

Generally, the knowledge economy underscores the significance of information technology in matters of production, economy, and society as well as the volume of human capital engaged in the generation of new ideas, innovations and technologies. Due to their implications, it has been mentioned that functional regions will differ not only in terms of their production of, and access to technological knowledge, but the mix of technological knowledge will also be different between functional regions; thereby making the important elements of production of technological knowledge to lean towards regional rather than national orientations.

In their work, '*Towards a Dynamic Theory for the Spatial Knowledge Economy*', Karlsson and Johnsson provided a perspective to theoretical understanding of knowledge economy by tracing it to the endogenous growth theory.

This theory places more emphasis on the role of the stock of accumulated knowledge and the growth of this stock in a given region.[7] By implication, it extended the arguments of Dasgupta & Stiglitz; Kamien & Schwartz[8] that market structure and nature of innovation activities are endogenous; as they both depend on factors such as Research and Development, technology, demand conditions and the nature of capital markets.

Karlsson and Johansson added that it is the size of the regional market potential that determines the probability that new knowledge in the form of inventions will be turned into innovations. They further argued that the underlying reason is that a large market potential increases the demand for knowledge intensive products. The probability of turning inventions into innovations can be assumed to increase with the size of the region, and this gives knowledge creating and knowledge using firms an extra advantage of locating in large regions.

In addition, when more knowledge creating and knowledge using firms locate in the large regions, this makes these regions more attractive for knowledge workers, and this fuels the cumulative process. They conclude that, as

6 Castells, Manuel (2004 b), page 312

7 Karlsson Charlie and Børje Johansson, Towards a Dynamic Theory for the Spatial Knowledge Economy, CESIS, The Royal Institute of Technology Center for Excellence for Studies in Science and Innovation (CESIS) Electronic Working Paper Series, paper No. 20, page 8. Available at: http://www.infra.kth.se/cesis/documents/WP20.pdf, accessed on September 14, 2007.

8 Karlsson and Johansson, supra, page 15. Citing, Dasgupta, P. and J.E.Stiglitz (1980), Industrial Structure and the Nature of Innovative Activity, Economic Journal 90, 266-293; Kamien, M.I. and N.L. Schwartz (1982), Market Structure and Innovation, Cambridge; Cambridge University Press.

the market potential of a region expands, the attractiveness of the region continues to grow.[9]

Beyond this economic commentary, a business dimension has been added to the theoretical explanations for the knowledge economy, making the EUi2010 initiative a product of processes designed to strengthen economic objectives pursued under a larger European integration.

There have been assertions that seek to provide insight into the theoretical foundations of EU initiatives. They include those of Manuel Castells for example, who asserts that such initiatives represents an alignment between two broad interests (a) that of large European firms struggling to overcome perceived competitive advantages in relation to Japanese and US capital and (b) that of state elites seeking to restore at least, part of the political sovereignty they had gradually lost at the national level as a result of growing international interdependence.[10]

Castells argues that on both counts of business interests and political interests, what was sought for was not supranationality, but the reconstruction of nation-based state power at a higher level, at a level where some degree of control of global flows of wealth, information, and power could be exercised.

He further points out that, *«the formation of European Union was not a process of building the European federal state of the future, but the construction of a political cartel, the Brussels cartel, in which European nation-states can still carve out, collectively, some level of sovereignty from the new global disorder, and then distribute the benefits among its members, under endlessly negotiated rules. This is why, rather than ushering in the era of supranationality and global governance, we are witnessing the emergence of the super nation-state, that is of a state expressing, in a variable geometry, the aggregate interests of its constituent members.»*[11]

Technological evolution continues to re-define the patterns of relations between governments; and between governments and individuals even though nation-states would continue to explore different forms of alliances.

Poulantzas Nicos in 1978, gave a description of how the modern nation is the product of the state; and warned that *'what is specific to the capitalist state is that it absorbs social time and space, sets up the matrices of time and space, and monopolizes the organisation of time and space that become, by the action of the state, networks of domination and power.*'[12]

---

9 Karlasson and Johansson, supra, page 13.

10 Castells Manuel (2004 b), page 328-329. Citing Streeck and Schmitter (1991:148)

11 Castells Manuel (2004 b), page 329.

12 See generally, Castells Manuel (2004 b), page 303.

Later in 2004, it was argued that such description was no longer the case and instead, what was taking place was that:

> *«State control over space and time is increasingly bypassed by global flows of capital, goods, services, technology, communication and information.»*[13]

Castells once again emphasised the basic challenge as being *'plural identities as defined by autonomous subjects'* that have been made possible by technology.[14] He further argued that the very existence of these challenges triggered a number of strategic responses shaped by the power relationships existing in and around political institutions.

The EU has continued to respond to this challenge since 1997 when it began the process of utilizing the benefits of the knowledge economy.

In the *'Green Paper on the Convergence of Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation: Towards and Information Society Approach'*, the European Commission pointed out the significance of an objective regulatory framework when it noted that:

> *«If Europe can embrace these changes by creating an environment which supports rather than holds back the process of change we will have created a powerful motor for job creation and growth, increasing consumer choice and promoting cultural diversity. If Europe fails to do so, or fails to do so rapidly enough, there are real risks that our businesses and citizens will be left to travel in the slow lane of an information revolution which is being embraced by businesses, users and by governments around the World. Governments and policy makers will have a key role in ensuring that such an environment is in place.»*[15]

The vision of the EU during this period was a steady march towards Knowledge Economy and the foundation as well as point of departure for this journey at the time, was represented by these basic services:

- Home-banking and home-shopping over the Internet,
- Voice over the Internet;

13 Castells, Manuel (2004 b), page 303
14 Castells, Manuel (2004 b), page 303
15 See COM (97)623, available at: http://ec.europa.eu/avpolicy/docs/library/legal/com/greenpaper_97_623_en.pdf, accessed on September 14, 2007.

- E-mail, data and World Wide Web access over mobile phone networks, and the use of wireless links to homes and businesses to connect them to the fixed telecommunications networks;
- Data services over digital broadcasting platforms;
- On-line services combined with television via systems such as Web-TV, as well as delivery via digital satellites and cable modems;
- Webcasting of news, sports, concerts and of other audiovisual services.[16]

Nonetheless, while in pursuit of an adequate theoretical explanation, Karlsson and Børje points out that *«the emerging knowledge economy has attracted much interest among economist and generated many important contributions during the last two decades. However, the literature does not provide a comprehensive picture and we are indeed lacking a «general theory»* of the knowledge economy. Various aspects of the emerging knowledge economy have been thoroughly analysed both theoretically and empirically but the overall synthesis is not yet present. It would be desirable to have a coherent theoretical framework that can explain how growth-induced investments in knowledge production stimulate localised, entrepreneur-driven innovations, which generate structural change and economic growth in an integrated system of functional regions. An interesting observation is that many of the necessary building blocks already seem to exist but that they are still waiting for someone to integrate them. The current state-of-the-art also includes inconsistent components.[17]

The foregoing theoretical and empirical notes contributed, to a significant extent, in articulating a framework for Europe on the Knowledge Economy and the Information Society. The product of such exercise is the issuance of a comprehensive strategy under the EUi2010 initiative, to boost job creation and growth within the region and achievable through the interaction between technology, the globalization of the economy and communications, politics, and political institutions.[18]

EUi2010: European Information Society 2010

The EUi2010 represents a five-year strategy from 2005 to 2010, adopted by the European Commission on June 1, 2005; designed to boost the digital economy of Europe.

16 Ibid.
17 See generally, Karlsson Charlie and Johansson Børje, supra.
18 Castells Manuel (2004 b), page 305.

It is a follow up to the Lisbon Agenda of 2000, which provides a comprehensive framework for the European Union and its member states Information and Communications Technology Policy.

A subsequent regional initiative, known as the eEurope 2002, ran from 2000 to 2002, having set the foundational policy objectives to stimulate the use of a cheaper, faster and more secure Internet. Its main focus was on connectivity; that is, getting people on line.

An addition to the overall policy objective was the need for higher adoption of broadband and other ICT services. It was also focused on providing a favourable investment environment, modernising public services and e-inclusion.

There have been other international initiatives along this policy concerns such as the UN General Assembly *Resolution 56/183 of 21 December 2001,* which endorsed the convening of the World Summit on the Information Society (WSIS) in two phases.

The first phase of the summit took place in Geneva from 10 to 12 December 2003 while the second phase took place in Tunis, from 16 to 18 November 2005.

The EUi2010 is a continuation of these regional and international initiatives with an adjusted focus in the context of the revised Lisbon Agenda. EUi2010 is required to shape the EU ICT policy until 2010. Prior to approval by EU member states by the end of the 2005, the member states were required by the Commission to define national information society priorities as a contribution to the objectives of EUi2010.[19]

Significance of EUi2010

The relevance of EUi2010 is indicated in the Commission's communication of 1st June, 2005.[20]

Three policy priorities were outlined under specific headings as follows:

- To create an open and competitive single market for information society and media services within the European Union. To support technological convergence with 'policy convergence', proposing further: an efficient spectrum management policy in Europe (2005); a modernisation of the rules on audiovisual media services (end 2005); an updating of the regulatory

19 See: http://www.eurescom.de/message/messageOct2005/i2010_The_EUs_new_ICT_strategy.asp, accessed on September 14, 2007.

20 IP/05/643, see : http://ec.europa.eu/information_society/eeurope/i2010/docs/press_release_en.pdf, accessed on September 14, 2007.

framework for electronic communications (2006); a strategy for a secure information society (2006); and a comprehensive approach for effective and interoperable digital rights management (2006/2007).
- To increase EU investment in research on information and communication technologies (ICT) by 80%. It noted that Europe lags behind in ICT research, investing only 80 Euro per head, as compared to 350 Euro in Japan and 400 Euro in the US. The i2010 further identifies steps to put more into ICT research and get more out of it, for example, by trans-European demonstrator projects to test out promising research results and by integrating small and medium sized enterprises better in EU research project.
- To promote an inclusive European information society. To close the gap between the information society «haves and have nots», the Commission will propose: an Action Plan on e-Government for citizen-centred services (2006); three «quality of life» ICT flagship initiatives which are represented by technologies for an ageing society, intelligent vehicles that are smarter, safer and cleaner, and digital libraries making multimedia and multilingual European culture available to all (2007); and actions to overcome the geographic and social «digital divide», culminating in a European Initiative on e-inclusion (2008).

As laudable as the EUi2010 initiative appears, caution in approach was proposed even as most countries welcome the strategy. In reference to a CNET report, the British IT trade association group, Intellect, observes that failure to get i2010 right could see Europe fall even further behind China and India as a competitive technology force.

A further caveat was that the «*…support for EUi2010 is tempered by a concern that only lip service is paid to the need for policy convergence, and … calls to action are guided by this concern.*»

In a white paper, Intellect further came to the conclusion that «*In order for the vision of EUi2010 to be realised, the European Commission and member state Governments must work with industry across the converged value chains. Success will depend upon moving beyond the silos of the old vertical markets.*»

Adding that «It remains to be seen how the Commission will manage to integrate the differing views of industry and national governments on ICT development in the i2010 strategy.[21]

21 See generally: http://www.eurescom.de/message/messageOct2005/i2010_The_EUs_new_ICT_strategy.asp, accessed on September 14, 2007.

Part 2

The theories of knowledge economy including those that influenced the EUi2010 provide a region specific foundation for designing a framework that is capable of responding to the information society and traditional system under global competitive pressures. The response from Europe through EUi2010 would encourage different responses and adjustments at different times BUT, along different lines of action; depending on the culture, level of development, institutions, and politics of each society.[22] However, the response from a developed country or region would necessarily be different from that of a developing country like Nigeria due to the complex nature of the needs of the latter.

Nigeria's Needs

It would have been easy to say that Nigeria's major challenge is that of getting people connected; and remaining connected both within itself and with the outside world. But this is only one of the country's many needs. It is however considered that a vibrant communications sector would facilitate durable solutions to the complex problems which afflict the nation.

To understand Nigeria's requirements, it is instructive to consider the areas of priority that have been identified by the nation itself, as representing its needs. I shall quickly refer to a fundamental document, the Kuru Declaration, issued in 2001, shortly after the 1999 transfer of power from the military back to civilians.

The document's first principle states:

> *« We adopt the New Orientation as an agenda for dealing with immediate and future issues of governance in Nigeria; removing impediments to efficiency and effective implementation and execution of programmes initiated by the federal government; expeditious actualization of government objectives and vision of national renewal and re-construction»*[23]

The tenth principle further states:

> *« We shall mobilize, involve and promote the interest of all stakeholders, namely, the society in general, since, in the ultimate, all decisions and actions*

22 Manuel Castells (2004 b), page 316.

23 See, 'Meeting Everyone's Needs', (2004) Nigerian National Planning Commission, page 5, available at: http://siteresources.worldbank.org/INTPRS1/Resources/Nigeria_PRSP(Dec2005).pdf, accessed on September 25, 2007.

of government are primarily concerned with promoting the security and general well-being of the people. There is also the need for a new attitude that has that concern permanently in focus, as the only goal, and that the economic well-being of all citizens in a truly democratic environment is of cardinal importance»[24]

To say that 'development' is what Nigeria needs, will not be overstating the matter. This is because, subsequent initiatives after the Kuru Declaration have continued to rehash these challenges which is also contained in the current administration's seven point agenda as follows:

- observing the rule of law,
- promoting job-led growth,
- ensuring distributive justice,
- enabling the poor and disenfranchised to link to the financial and capital markets,
- providing the requisite environment for foreign and domestic investment in critical infrastructure, for example, transport,
- massive intervention in education, and;
- a plan to tap the considerable wealth and experience of Nigerians in the Diaspora[25].

With the aspiration of Europe towards the knowledge economy and the framework for its attainment as articulated under EUi2010 initiative, Nigeria undoubtedly shares the same goal; only that it still struggles to avail itself of the benefits of information and communications technology.

But this similarity of goals would be better appreciated if it is considered in relation to issues such as (a) the different stages of development between Europe and Nigeria; (b) challenges of governance with effective administration of public-focused policies and laws in a developing country; (c) capacity to resist external pressures to apply uncritical and un-examined policies; and (d) the ability of being self-deterministic, especially, regarding priority areas of government policy objectives.

The significance of the contrasts between Europe and Nigeria with the foregoing factors as background is significant for priority setting and need for effective regulatory administration in each country; especially given the fact that European Union comprises of 27 developed countries located in a developed

24 See, 'Meeting Everyone's Needs', (2004), supra, page 5.
25 See: http://odili.net/news/source/2007/sep/16/306.html, accessed on September 18, 2007.

continent; while Nigeria is a developing country located alongside 52 other developing countries, within the African continent.

Additional contrast is that the EUi2010 was adopted in 2005 which was two years after the Nigeria Communications Act was enacted. The significance of the Nigeria Communications Act of 2003 is that Nigeria can not be said to have attained the level of technological growth or even close to achieving availability and quality in basic communications services.

It does not matter whether the yardstick for such evaluation is 2005 when EU was already prepared to move to the next level of knowledge economy with the EUi2010; or at present, 2007, when networks have difficulties linking up subscribers in Nigeria. Worse still, it should be noted that the stage where Nigeria is at the moment is far behind where Europe was as at 1997, when the Green Paper was issued, to promote wider geographical reach of basic communications services.

It would have been desirable to immediately witness the opportunities that EUi2010 promises for Europe being replicated in Nigeria; but Nigeria requires first of all, to lay the basic foundations of integrating an effective process in the regulatory and administrative framework that will sustain overall benefits from the communications sector.

Presently, Nigeria requires comprehensive and effective processes that can secure the Millennium Development Goals (MDGs). These goals, as represented under MDGs, are similar to those dreams which Nigeria have articulated over the years not only in the Kuru Declaration but also in legal instruments and documents such as:

- Vision 2010 report,
- Nigeria Communications Act, 2003,
- National Economic Empowerment and Development Strategy (NEEDS) 2004,
- National Telecommunications Policy (NTP),
- Vision 2020, (a target of being among the top 20 economies in the world by that date),
- Seven-point Agenda (issued after May 29, 2007).

Apart from the National Telecommunications Policy which was followed by the enactment of the Nigeria Communications Act of 2003, all other documents do not have Information and Communications Technology (ICT) as their central focus. However, one similarity that all these instruments and documents have in common is that none has been translated into reality in accordance with their fundamental objectives.

With all the declarations and documents still unmet, adapting a new document in the nature of EUi2010 into the mix, even under a certain regulatory framework, would be an effort that ignores pre-condition of basic foundation on which something durable can be built. Additionally, the factors of locality and particularity will not make such an approach any easier. Put differently, a framework would require reflecting (a) basic or necessary foundation prior to laying down the framework and (b) ensuring localised and indigenous realities are considered or else it would not only be diversionary but could lead to effort in futility. The frustration is easily captured by a situation which George Ayittey describes as a 'meretricious fandangle of imported system which the elites themselves don't understand'[26]

The pillars for Nigeria's ICT development that is capable of sustaining the country's economic sectors had been provided not only through policy and laws but with an even more recent exploit in Nigerian Communications Satellite 1 (NigComSat-1).[27] The NigComSat1, as it is presently referred, was launched by China on behalf of Nigeria on May 13, 2007 being the product of contract signed in December 2004 at a reported cost of about 400 million US dollars. It consequently adds up with an earlier project, the Earth Observation Satellite, NIGSAT-1, which was launched from Russia in 2003.

Even as the recent project would be considered as an investment that the government considered necessary for the country's participation in the information society and utilization of the knowledge economy, it was nonetheless faulted by some observers. In this connection, an editorial in a national daily's notes that:

> *«the satellite is a right step taken at a wrong time» … while it points out that «the satellite projects are noble but there is nothing on ground that would enable the country benefit»*[28]

It further adds that: «We are amazed that credible institutions like the Nigeria Academy of Science were not carried along ab initio in the conceptualisation and implementation of the communications satellite project … if we are to achieve any meaningful development.»

---

26 See, Ayittey George 'George Ayittey: Cheetahs vs. Hippos for Africa's future' available at: http://www.ted.com/index.php/talks/view/id/151, accessed September 19, 2007.

27 See: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/13/AR2007051301264.html, accessed on September 19, 2007.

28 See 'The Daily Independent' editorial available at: http://odili.net/news/source/2007/jul/3/614.html, accessed on September 19, 2007.

Another earlier effort before the preceding ones was the substantial investment made by Nigeria in South Atlantic 3 / West African Submarine Cable (SAT-3/WASC), through its former monopoly Nigeria Telecommunications Limited (Nitel)). The SAT-3 in issue, comprise of submarine communications cables, which were expected to fast track development through information and communications services. SAT-3 links Portugal and Spain to South Africa with connections in other West African countries, along that route.It is regrettable though; that all these substantial public investments have not been efficiently utilized to improve prospects of development and the benefits of quality communications services so as to narrow the digital divide, from within Nigeria.

The shortfall in expectations recently drew the attention of participants at SAT-3 workshop taking place in Abuja, Nigeria on September 13, 2007. A special concern was on the market structure that accounts for high prices in which for example, SAT-3 bandwidth in the African countries cost between $4,500 and $12, 000 per Mbit/s per month, compared to what operates in other countries (US). The Nigeria Minister of State, Information and Communications, (Alhaji Ibrahim Nakande) used the opportunity to renew calls for the development of GSM roaming facility in the West African sub-region.

Adding this to the string of contrasts between Nigeria and EU, as noted earlier, it illustrates a more troubled sector. Especially when considering that while there is absence of GSM roaming facility within the 15 member countries of Economic Community of West African States (ECOWAS), the EU Commissioner for Information Society and Media, Vivian Redding had already completed a plan of action that reduced roaming charges for voice calls in EU. This EU line of action was to ensure that consumers crossing borders within the EU are not compelled by network tariff models to pay higher roaming fees.[29] Having achieved success with voice calls, the EU has made it known that it will still embark on regulatory action aimed at a further reduction in charges for text messaging and data usage generally.[30]

The slow process in the Nigeria ICT sector is obvious; and it is becoming increasingly difficult for public officers to remain indifferent as the sector appears to have provided an experimental arena for both the operators and regulatory authorities.

29 See: http://networks.silicon.com/mobile/0,39024665,39159527,00.htm, accessed on September 14, 2007.

30 See, 'Next in EC's Sight: Data Roaming Charges', available at: http://www.businessweek.com/globalbiz/content/jul2007/gb20070723_115750.htm, accessed on September 16, 2007.

An insight into this situation is not far-fetched as can be further discerned from a recent event.

While inaugurating the Nigeria's Senate Committee on Communications on September 14, 2007, the Senate President frowned at the conducts of operators' refusal to appear before the National Assembly's Committees. He referred to such conduct as irresponsible and criminal. The Senate president declared that henceforth, strict sanctions would be enforced against any Chief Executive Officer «who would flagrantly avoid an invitation coming from the Senate of the Federal Republic of Nigeria without giving a convincing reason for doing so.»

Similarly, during his opening address, the Chairman of the newly inaugurated Senate Committee on Communications (Senator Sylvester Anyanwu) expressed with dismay that in spite of the gains offered by the deregulation of communication sector, the sector was «still grappling with series of service problems to the chagrin of all and sundry.»

The Chairman observed that «Even though the subscriber level in the country has reached a whopping 40 million, the tariff is still high, while the percentages of call completion rates and dropped-calls have given Nigerians serious head and heartaches.»

He noted further that the question of poor quality of service by GSM service providers had engaged the attention of the senate since 2003, and that only recently; he had sponsored a motion on the increasing rate of dropped-calls due to inefficient GSM network in Nigeria. The Senate Committee Chairman emphasised that …

> *«…records available to our committee show that a particular contractor has been paid full amount of total contract sum before it commenced actual work on the project and this is quite disheartening, particularly when major contractors handling the Rural Telephony Project are foreign companies...», while warning that the Senate must not allow the boom brought by communication to be turned into a doom for Nigeria.*[31]

One can compare the above commentary on operators in Nigeria through the concern of its law makers on one hand, and on the other hand, a typical communications problem that was experienced in Norway only a couple of

31 See Sun Newspapers editorial of September 14, 2007: 'Senate set to slash GSM charges, sanction defaulters' available at: http://odili.net/news/source/2007/sep/14/812.html, accessed on September 15, 2007.

weeks ago when Telenor subscribers had their conversations disrupted, due to faulty network.

As the problem persisted, even though Telenor claimed the problem had been resolved, the stern warning from Datatilsynet, a supervisory agency, did not leave Telenor in any doubts as to the nature of sanctions that will follow if they did not clear up the problem.[32]

Information and Communications Technology present a great opportunity to attain development but it requires efficient regulatory process that commences at ensuring existence of fundamentals or basic communications services, which are not even yet available in Nigiera as they should. The regulatory management of the communications sector is required to be focused on serving the society's common good. The expansion of the public space through communications provides a base for sustainable increase in the national production, capable of propelling the journey to a modern economy.

Without establishing the institutional and infrastructural foundations to realise basic services, it will be a challenge to adopt a framework that is soon disregarded due to complexity, in hope of achieving technological advancement in a short while.

Conclusion

A few lessons do exist in the contrasts. For example, much as the main objective of EUi2010 is to boost jobs and growth, it is to be noted that the success or failure of this initiative would not exclude Europe from the network society. Nigeria, however, strongly desires to be connected to the network society; for purposes of improving people's quality of life as well as facilitating a wider participation of its people in economic, democratic and other essential societal processes.

Further, European Union is not only a developed region; it has also attained significant level of development before seeking ways of consolidating its progress in knowledge economy through EUi2010 initiative. For Nigeria, the communications sector provides a credible path for Nigeria, to attain its development objectives.

Given Nigeria's population of approximately 140 million, including an appreciable geographical spread, a regulatory framework that adequately meets Nigeria's needs would first of all, ensure that basic services are put in place and rigorously sustained to meet societal expectations.

32 See, 'Datatilsynet –Telenor må rydde opp snarest' available at: http://www1.vg.no/teknologi/artikkel.php?artid=162939, accessed on September 18, 2007.

The limitations to this reality in Nigeria remain the country's unregulated market strategy in the communications industry; lack of a functional competition authority; and absence of unified regulatory structure for communications sector. These limitations have combined to diminish the country's prospects of maximizing the benefits of ICT so soon as would have been necessary.

In essence, Nigeria requires a focused and effective communications regulation framework that can stimulate socio-economic and political development in accordance with sector's policy and law specifications. In the absence of a framework that guarantees basic services, the limitations and peculiar conditions in Nigeria would make the application of EUi2010 a misplaced priority for the country at this stage of its development.

DEFINING LEGAL RISK*

Tobias Mahler

Abstract:

What is legal risk? This category of risk is often mentioned in the context of enterprise risk management and financial risk management. However, the definitions given for legal risk differ widely, and no generally accepted notion of legal risk seems to exist. Moreover, many existing definitions of seem to build on an insufficient understanding of the concept of law. The objectives of this paper are to review, systematize and analyse existing definitions of legal risk. This paper proposes a context-independent definition and classification of legal risk, based on norm theory.

1 Introduction

Risk is a historically rather new phenomenon. The modern conception of risk is rooted in the Hindu-Arabic numbering system that reached the West seven to eight hundred years ago (Bernstein 1996). Risk could not be understood properly without the probability theory developed during the Renaissance. Today, the concept of risk is the key element in risk management. The latter term refers to a set of coordinated activities to direct and control and organisation with regard to risk (ISO 2002). Recent years have seen an increase in focus on risk management in many disciplines. Sectors such as enterprise management (COSO 2004) and banking (Basel Committee on Banking Supervision 2006, hereinafter Basel II) have developed targeted frameworks to manage risk.

In law, the first use of probability theory dates back to Leibniz's dissertation of 1665 (Bernstein 1996, p. 57). Nevertheless, we are today still struggling with the relationship between risk and law. Not only do we need to understand how the law should deal with risk (e.g., Steele 2004). In addition, there are developments towards introducing risk management as a method to be used by lawyers (e.g., McCormick 2006, Wahlgren 2003, Keskitalo 2000).

* This paper is based on a presentation the author gave at the conference "Risk and Regulation 2006" at the London School of Economics and Political Science (LSE), organized by the Centre for Analysis of Risk and Regulation (CARR). An earlier version of this paper was presented at the conference «Commercial Contracting for Strategic Advantage – Potentials and Prospects», Turku University of Applied Sciences, June 13-16, 2007.

However, so far, methodologies for legal risk management are still «in their infancies» (Burnett 2005).

Legal risk management can be defined as a methodology which consists of activities to manage a particular set of risks, namely (1) legal risks and (2) risks that can be «treated by legal means» (Mahler and Bing 2006). *Legal risk* is thus a key element of legal risk management, but the term is used in many different ways and deserves further analysis. This paper's objectives are to review, systematize and analyse existing definitions and classifications of legal risk. This paper submits that a successful understanding of legal risk needs to be informed by theories on the concept of law. Therefore, this paper will introduce a context-independent classification of legal risks, based on norm theory.

The most authoritative definition of legal risk is probably the rather loose understanding included in the Basel II accord:

> *«Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements» (Basel Committee on Banking Supervision 2006, footnote 97).*

This definition will probably have a major influence on the understanding of legal risk in the Basel II-related Banking Directive (Article 4 (22) of 2006/48/EC), which provides no definition. The banking sector has been particularly interested in the definition of legal risk and has produced many incoherent definitions. This interest in defining legal risk seems to have arisen somewhat accidentally when the banking sector endeavoured to define different types of risks relevant to banks. There are many different definitions of legal risk, but most seem to fall into one of the following two groups. The first set of definitions links legal risk to *legal uncertainty*. Most other definitions define legal risk by giving a number of examples, which include, in addition to legal uncertainty, *uncertainty about factual elements*.

The definition of legal risk should distinguish legal risk from other types of risk. A starting point for this definition is the intersection between, respectively, the concepts of law and risk as illustrated in Figure 1. In addition, it will improve our understanding of legal risk if we can *categorize* the different types or forms in which legal risk materializes. We will adopt an approach put forward by McCormick 2006), who distinguishes *two types of legal risk*. McCormick fails to explain what, exactly, distinguishes and delimits these two types of legal risk; he seems to follow his intuition. As this paper shows, however, this distinction is in line with norm theory, which provides a relevant reference framework from which to analyse the relationship between legal norms and risk. This typology can then be further refined by adding the dimensions of

factual and legal uncertainty, thereby creating a basic set of four types of legal risk, as illustrated in Figure 1. The distinction between these four types of legal risks is clarified in Section 5.2.3 at the end of this paper.

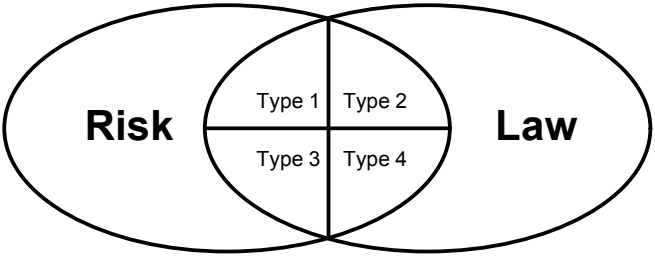


Figure 1 – Legal risk as the intersection of risk and law

Of course, we may ask, «Why do we need to define and categorize legal risk?» Some writers argue that legal risk is a rather loose category, which does not need to be defined, and which is essentially context-dependent. Some even consider it unworthy to devote much attention to definitions of risk:

> *«It is […] generally agreed that not too much attention needs to be paid to questions of definition, for definitions serve only to delimit, not adequately to describe (let alone explain), the object under investigation» (Luhmann 1993, p. 7).*
>
> *«There is no standard definition of legal risk and it may not be very helpful to produce one… It is simply risk which lawyers can help to identify or mitigate» (Kenny 2004/2005, p. 22).*

However, valid reasons justify devoting some thought to the definition of legal risk. We face a situation in which different actors, even within the same business sector, define legal risk inconsistently, which, in itself, is unsatisfactory. Moreover, the recently adopted Banking Directive uses the term legal risk, and this use must have a specific meaning. Finally, if it is possible to define a kernel that can form the conceptual basis for any sector-specific use of the term, then this should greatly simplify communication across different sectors.

To call any risk a legal risk, just because *lawyers can help to identify or mitigate* it, would be too wide. On one hand, many lawyers understand themselves as generalists and may help their clients to identify and mitigate non-legal risks, as well as legal risks. On the other hand, a «legal measure,» e.g., the adoption of an additional contractual clause (e.g., *force majeure*), may be used

to mitigate a risk that could be called a legal risk only with difficulty (e.g., the inability to fulfil a contract as a *consequence of an earthquake*). Thus, legal risk management should be understood to deal with two types of risk, which lawyers can help to identify and mitigate: (1) legal risks and (2) risks which can be mitigated by legal measures.

The remainder of this paper is structured as follows. Section 2 introduces the *methodology* used to define and to classify legal risk. In essence, the paper combines descriptive and prescriptive approaches to legal risk. Subsequently, Section 3 concentrates on the concept of *risk*, which is core to the understanding of legal risk. Then, Section 4 describes how *legal risk* is understood quite inconsistently, and discusses how it could or should be *defined*. Section 5 discusses the possibility of classifying different types of legal risk. Practical typologies will be contrasted with a proposed *norm-theoretic classification*. Finally, Section 6 draws this paper's *conclusions* and provides a first indication of how the concept of legal risk can be used in legal risk management.

2 Methodology

In order to understand legal risk we address both the definition and typological classification of legal risk. The question of definition can be asked in two ways: a) How *is* legal risk defined and what is meant when practitioners *use* the term legal risk?, and b) How *should* the term be understood and used? Similarly, the possibility of drawing up stable categories or types of legal risk can be looked at from two perspectives: a) What typologies of legal risk *are* used and suggested, e.g., in the literature?, and b) How *should* we classify types of legal risk? Table 1 illustrates how these different perspectives are used in this paper.

Legal risk	Descriptive	Prescriptive
Definition	Section 4.1	Section 5.1
Typology	Section 4.2	Section 5.2

Table 1 – Descriptive and prescriptive approaches in this paper

2.1 Defining legal risk

What should be the preferred method to define legal risk? The traditional Aristotelian approach is to define a species *per genus et differentiam*. As an example, humans might be defined as animals (the genus) having the capacity

to reason (the differentia) (Smith 2006 (Winter Edition)). In the context of this paper, the *genus* could be risk, and the criterion which differentiates it from other risks is the adjective «legal.»

> *This Aristotelian approach has some limitations, which were pointed out by, e.g., Wittgenstein. For example, it may not be possible to find common features for, e.g., all games (Wittgenstein 1997, section 66; Eng 2003, 85–102), but rather partial and overlapping resemblances. It remains to be seen if this limitation also affects the concept of legal risk, i.e., if we can identify common features for all legal risks. The combination of the substantive «risk» and adjective «legal» seems to indicate that we should understand legal risk as a type of risk, which is to be distinguished from other types of risk. This is exactly the per genus et differentiam approach. Thus, the semantic context provides a preliminary indication that the methodological starting point for this study should be the above mentioned Aristotelian approach. Of course, this may be complemented by alternative approaches (see Eng 2003, p. 91) in case the proposed strategy fails to succeed in practice.*

This paper analyzes the definition of legal risk from descriptive and prescriptive[1] perspectives (see further Kolflaath 2004, p. 104). The *descriptive approach* analyses how legal risk is understood by literature and practice. The evidence used for this part of the investigation consists of definitions of legal risk in books, journals, reports, etc. by banks, lawyers, economists, risk management practitioners, etc. Evidence of how companies use the term legal risk in practice is more difficult to obtain, and has been considered to a minor degree. Because the descriptions and evidence of the use of the concept form a heterogeneous material, we can expect these semantic uses to both contradict and complement each other.

The second perspective taken here is a *prescriptive* approach, which deals with how legal risk should be meaningfully defined. By definition we mean a proposition which contributes to normatively determining the meaning of a linguistic entity (Eng 2003, p. 28). The method of definition depends on the answer to the following question. Is legal risk a concept we *construct* as we find suitable, or is it a phenomenon we can *observe and describe based on evidence of legal risk in the outside world*? The latter alternative can be

1 An alternative wording for «prescriptive» would be «normative». However, the latter wording is avoided here in order to avoid confusion with the use of «normative» in the context of norm theory addressed in this paper.

chosen only if we can determine what should constitute evidence of legal risk. However, no such evidence seems to exist. There is evidence only of how relevant actors perceive and describe their situation. Risk is not an observable phenomenon, but a «self-produced» social construct. This has already been observed by Luhmann:

> *«The outside world knows no risks, for it knows neither distinctions, nor expectations, nor evaluations, nor probabilities – unless self-produced by observer systems in the environment of other systems» (Luhmann 1993, p. 7).*

Hence, the *concept of risk* is (prescriptively) constructed to suit the needs and requirements of planning for an uncertain future. In practice, we seek to align our concept of risk with the term's established use in risk management. The adjective «legal» in our compound notion merely adds to risk the perspective of law. Thus, the definition of legal risk must also be pragmatically constructed suitably and usefully.

We need some clear criteria to guide this pragmatic construction. The following requirements will be applied to shape a prescriptive definition (Kolflaath 2004, pp. 79–92): First, a definition should clarify the meaning of the defined term in the relevant context. Second, a definition should provide a scope which is neither too wide nor too narrow. Third, the definition should facilitate and optimize decision-making based on the definition.

2.2 Typology of legal risk

Once the meaning of the term «legal risk» is clarified, we are interested in understanding the different types of legal risks. This question deals less with semantics than with a classification of different manifestations of legal risk. Each class or type of legal risk can be defined in the way discussed above. Hence, we can use the criteria for prescriptive definitions presented above (i.e., clarify the meaning, optimize the width of scope and facilitate decisions). In particular, we will focus on facilitating a clear decision about which type of legal risk a particular situation belongs to. This is best achieved if the different types of legal risk are mutually *exclusive*, i.e., a single risk cannot be categorized as two types of risk.

In addition, we are interested in exhaustiveness. When a typology is *exhaustive*, it is complete in the sense that it covers all cases or possibilities. Exhaustive typologies imply more stable knowledge, but can be falsified if even a single example is not covered by the typology. Any non-exhaustive

typology is of more limited value, as it implies only a minor advance from a mere collection of examples.

Hence, existing classifications of legal risk are reviewed and analysed in order to get an understanding of how legal risk materializes and how it can be recognized. The paper then proceeds to suggest an exhaustive typology of legal risk which consists of two types of legal risk. These types are, under certain conditions, mutually exclusive. This proposal is based on norm theory, which provides us with types of norms that are relevant regardless of the factual or legal context.

3 Risk

The concept of risk has been studied in different disciplines based on varying definitions. In principle, the concept of risk has the potential to be a «transdisciplinary field» (Luhmann 1993, p. 6), comparable to, e.g., systems theory. However, this potential has not yet been fully realized, partly due to the lack of a common definition (Keskitalo 2000, p. 48f). According to the Stanford Encyclopedia of Philosophy (Hansson 2007), it is possible to distinguish at least five different definitions of risk, which are used across various disciplines. As Luhmann (ibid, p. 6) puts it:

> *«There is no definition of risk that could meet the requirements of science. It appears that each area of research concerned is satisfied with the guidance provided by its own particular theoretical context.»*

For the purpose of this paper, we are particularly interested in the relationship between risk and uncertainty, because legal risk often is understood as equal to legal uncertainty. Following Knight 1921), risk is often distinguished from «true uncertainty» by understanding risk as *probabilistically measurable uncertainty*. This distinction between risk and uncertainty was influential for decision theory, which commonly distinguishes decisions under risk from decisions under uncertainty. However, this leaves us with the question of what is probabilistically measurable. The traditional,[2] and rather pragmatic, answer is to reduce all uncertainty to risk through the use of beliefs expressible as probabilities (Mas-Colell, Whinston et al. 1995, p. 207). For example, if we are uncertain about the probability of falling from a bicycle on an icy road and wounding a knee, we use the cyclist's beliefs to assess the risk. Decision theory

2 Alternatively, we may seek to address the above mentioned «true» uncertainty by explicitly addressing our lack of information. See further, Ben-Haim 2006, p. 342.

often refers to this probabilistic method as a *Bayesian approach*, because it builds upon the mathematical models developed by Thomas Bayes (Hansson 2005, p. 37).

Notably, this distinction between risk and uncertainty features most prominently in decision theory. In other contexts, the distinction between risk and uncertainty often is understood along the *subjective-objective dimension*. Hansson 2007 uses the following example:

> *«Whereas 'uncertainty' seems to belong to the subjective realm, 'risk' has a strong objective component. If a person does not know whether or not the grass snake is poisonous, then he is in a state of uncertainty with respect to its ability to poison him. However, because this species has no poison, there is no risk of being poisoned by it. The relationship between the two concepts 'risk' and 'uncertainty' seems to be, in part, analogous to that between 'truth' and 'belief'.»*

3.1 Defining risk

As a point of departure for the present paper, we suggest the following ISO definition of risk, which is representative for the use of the term in risk management:

> *Risk is the combination of the probability of an event and its consequences (ISO 2002, definition 3.1.1).*

It is implicit in this definition that that the possibility of *negative* consequences at least exists (ISO 2002, note 1 to definition 3.1.1). In other words, the possibility of positive outcomes is no obstacle to the existence of risk. It is common to determine a value for each risk by combining the values of probability (e.g., in %) with the (e.g., monetary) value of the event's consequences. For example, a low probability of the event and a low consequence (e.g., loss) indicate a low risk.

Notably, this probabilistic concept of risk differs from the understanding of risk in law, in particular, contract law.[3] Lawyers do not typically assess probabilities when addressing risk. Instead, the question is, «*Whose* risk is this?»

3 We need to distinguish between, on one hand, how risk is (traditionally) understood by lawyers and, on the other hand, how we should understand legal risk. This section addresses the former question.

i.e., the concept implies that the parties to a contract «bear the consequences (loss) that result from certain contingencies» (Selvig 1965–1978, p. 144, see Keskitalo 2000, p. 51 f). The concept of risk in contract law is thus related to the question of risk allocation or bearing. Risk management takes a similar perspective in the context of *risk transfer,* where an identified risk is sought to be transferred to another entity. However, the key difference between the traditional legal understanding of risk and the risk concept developed above is the time perspective. The principal perspective of law is the judge's *ex post* viewpoint, after the event has materialized.[4] At this point in time, the question of the event's likelihood makes no sense (except in the special case of negligence). This is contrasted by the *ex ante* perspective of risk management (see further Keskitalo 2000, pp. 67–68), which was adopted in this paper.

3.2 Approaching legal risk through legal uncertainty

When approaching legal risk, we need to relate the two concepts of risk and legal norm. The concept of law is the topic of a wide range of literature (e.g., Hart 1994), and is well known to the legal discipline. In this paper we are particularly interested in the basic structure of law, which consists of legal norms (e.g., Eckhoff and Sundby 1988, pp. 43–60). Every legal norm consists of an antecedent (if A) and a consequent (then B). Antecedent and consequent are linked by a normative modality, which states *how* antecedent and consequent are related. For example, if A is the case, then there may be a legal *obligation* to perform B.

What does the concept of risk add to this legal perspective? The contribution of the risk perspective to law consists of at least the following three elements:

- First, risks involve (mostly) negative consequences of events. In order to know whether a legal norm has negative consequences, we need to apply the norm to a given set of facts and evaluate the result from the stakeholder's *subjective perspective* as either beneficial or detrimental for his assets or objectives.
- Second, risks imply *future* events, i.e., we need to assume an ex-ante perspective, different from the ex-post perspective of, e.g., a judge.

4 Of course, lawyers drafting contracts are the core exception, because they need to have a proactive perspective ex ante. The recognition that contract formulation and entry constitute an act of risk-taking is acknowledged, e.g., in the work of Sandvik 1966. See, for further examples of the risk discourse in jurisprudence, Keskitalo 2000, pp. 51-55.

- Third, risks entail *likely* future events, obliging us to address matters of *uncertainty*.

In the legal context there is a necessary basic distinction between two conditions of uncertainty of an event regulated by a legal norm. Every legal norm consists of an antecedent (if A) and a consequent (then B). If we assume that the consequent (B) is negative for the stakeholder, then we need to determine if the norm will «fire.» This depends on two questions, which are essential here: first, whether the set of facts (A) is or will be true; and second, whether the application of the norm to the set of facts (A) then renders the consequence (B). Uncertainty may prevail with respect to both aspects.

The norm's likelihood of firing may depend on *legal uncertainty*, e.g., if an obligation depends on the interpretation of the law. In addition, the likelihood of the norm firing depends on uncertain facts or conditions, which are described in the antecedent and which trigger the consequent of the norm. A judge, or anyone applying the norm, compares these conditions to the «facts» of the case. The uncertainty about these conditions described in the antecedent is hereinafter referred to as *factual uncertainty*. This distinction between legal and factual uncertainty, a key factor for understanding legal risk, is illustrated in Figure 2. For the purpose of this paper, we consider legal uncertainty and normative uncertainty as synonymous.

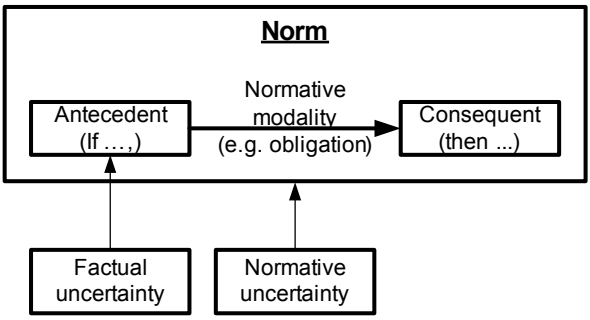


Figure 2 – Factual and normative uncertainty

However, there is a terminological difficulty with our use of the term «uncertainty» here. This difficulty stems from the combination of different perspectives in this paper. The term «legal uncertainty» does not build upon the distinction between (probabilistic) risk and (non-probabilistic) uncertainty in

decision theory. Concomitantly, we cannot necessarily extend that distinction to (probabilistic) legal risk and (non-probabilistic) legal uncertainty. Instead, legal uncertainty is used generally to denote that it is not fully known how the law regulates a given set of facts, even if we have a fairly clear idea of the probability of a particular outcome in a case. Similarly, factual uncertainty is used here to denote that the future set of facts is unknown in the present. Factual uncertainty will be used independent of whether or not the likelihood of these facts is probabilistically measurable. Nevertheless, this distinction between legal uncertainty and factual uncertainty proves practically useful, as will be seen below in Section 4.1 and in the following example:

Example 1: If a bank considers the risk of exposure to a fine for particular breaches of regulation, it needs to consider a number of uncertain aspects. The norm according to which the bank could be fined consists of an antecedent (if breach of regulation) and a consequent (then pay fine), which are linked by the normative modality (obligation). This consideration needs to include, first, the factual uncertainties regarding the antecedent. Particular (uncertain) market conditions may trigger the regulation's applicability. Moreover, it may be uncertain whether the bank's employees will abide by the regulation, once applicable. Second, even if the antecedent's conditions are fulfilled, there may be normative uncertainty about if and how much the bank will be fined. For example, in the case of a new and unproven penalty norm, the regulatory authority may have a considerable margin of appreciation. Thus, the bank will need to consider both normative and factual uncertainties.

The distinction between factual and normative uncertainty resembles, but should not be confused with, the duality of cognitive and normative expectations, which is a central concept in Luhmann's sociology of law. Luhmann 1972 (vol. 1, pp. 40–53) uses the term normative expectation to express that an actor is expected to abide by relevant norms. Such normative expectations are kept up, even though the expectation is sometimes frustrated. In this sense, the expectation is counterfactual. Thus, Luhmann uses this distinction in an entirely different context. Once we shift our focus from society's expectation about compliance (Luhmann) to an individual's consideration of uncertainty (this paper), we need to reflect about what makes the future uncertain. Luhmann's normative expectation being upheld, even if there is little evidence of compliance, does not reflect the considerations of the individual who depends on some actor's compliance. A real-life actor considering his risk exposure cannot disregard the uncertainty of other actors' compliance. Human acts are uncertain, and the law is one aspect which, at least potentially, influences

human behaviour. Factual uncertainty, as used in this paper, thus includes the question of whether or not an actor chooses to abide by the law (which is the topic of Luhmann's normative expectation), because the «fact» of law-abiding behaviour may be a relevant aspect in the antecedent of a norm. In the above example 1, Luhmann's normative expectation applies both to the bank employees, who are expected to abide by the regulation, and to the supervisory authority, which is expected to fine the bank only if and as far as the conditions of the penalty norm are fulfilled. However, Luhmann explicitly disregards the possibility of non-compliance, which cannot be excluded from a legal risk analysis. Thus, Luhmann's duality of expectations is not directly applicable in the analysis of legal risk.

4 Definition of legal risk

What is legal risk and how should it be defined? By «*definition*» we mean a proposition which contributes to normatively determining the meaning of a linguistic entity (Eng 2003, p. 28). The definition we look for is a proposition which contributes to normatively determining the meaning of the linguistic entity «legal risk.» The paper first approaches the meaning of the term by *describing* how others define legal risk. Subsequently, it discusses in a *prescriptive* perspective how legal risk should be understood.

4.1 Descriptive approach

It is not surprising that there are many definitions of legal risk. However, the definitions reproduced below indicate disagreement about the concept's most fundamental aspects.

4.1.1 Only legal uncertainty is legal risk

Legal risk is sometimes defined as the risk that is caused by, or which depends on, *legal uncertainty*. This can be illustrated by the following examples of definitions:

Legal risk: «The risk that unexpected interpretation of the law or legal uncertainty will leave the payment system or members with unforeseen financial exposures and possible losses» (Bank of England 2000, emphasis added).

[Legal risk] «arises through uncertainty in laws, regulations and legal actions» (riskdimensions.com , emphasis added).

A similar approach was taken by UNIDROIT, which described legal risk as «a situation where the applicable law does not provide for a predictable and sound solution» (McCormick 2006, p. 111). This definition includes legal uncertainty, but even encompasses a more general lack of quality of the law, which «does not fit the market reality.»

4.1.2 Legal and factual uncertainty

In the view of most writers, particularly within risk management, legal risk covers both legal and factual uncertainties. Admittedly, this distinction is normally not made explicit, but the examples clearly indicate that uncertainty about facts is not excluded from legal risk. The following section illustrates this with examples of the term's practical use, and with definitions provided in various documents.

Legal risk is sometimes addressed in companies' annual reports on finance and corporate governance issues. In some countries, including, e.g., Germany, risk management is an explicit duty of incorporated companies (§91 II Aktiengesetz), and the resulting reports provide useful insight into how companies manage their legal risks.

A broad review of the use of the term legal risk in companies' annual reports is neither possible nor useful within the scope of this paper. A report issued by the aerospace company EADS is employed here to illustrate and exemplify the difficulties in delimiting different types of risk in which legal issues play a role.

This report (EADS 2005) distinguishes four types of risk for this company, which is probably better known as a participant in major consortia such as Airbus and Eurofighter. These four types of risks are financial risks, business-related risks, legal risks and industrial & environmental risks. EADS does not define these categories, but uses them as the company sees fit. The risks covered under the heading «legal risks» are related to (i) the dependence on joint ventures and minority holdings, e.g., Eurofighter and Airbus, where the «risk of disagreement or deadlock is inherent in a jointly controlled entity»; (ii) product liability and warranty claims «in the event that products fail to perform as designed» and (iii) changes in export control and other regulations. What kind of uncertainties do these risks address? Interestingly, all risks depend on whether or not a set of facts will occur and not whether a legal norm will «fire.» Thus, the EADS report provides evidence that at least some practitioners do not understand legal risk as limited to legal uncertainty.

Moreover, another point is striking in the EADS report: it also discusses legal norms extensively in two of the three other risk categories. Business risks

include, for example, risks from «public-private partnership» (PPP) contracts. There is no definite reason to classify PPP contracts as a business risk, while including joint venture contracts as legal risks. Maybe legal risk is not a separate, distinguishable concept, but indicates only that risks are viewed in a legal perspective, which is one of many meaningful perspectives on risk.

The same conclusion could also be drawn from the many available definitions of legal risk. Many definitions of legal risk essentially employ examples as their only means to clarify the concept. This may be the case because the author is interested only in the specific example. Alternatively, it may indicate that the phenomenon is insufficiently understood or is considered too difficult to describe in the abstract. Notwithstanding, the examples given in literature and practice provide a useful insight into the variety of relations between law and risk. As will be shown, the definitions refer to both beneficial and detrimental norms.

a. Legal risk: «The likelihood that a trading partner will opportunistically breach a contract or expropriate intellectual property rights» (Hill 2005, glossary).

This example deals in its first part[5] with a situation in which the legal norm is to the benefit of the stakeholder, and where the uncertainty depends on the trading partner's actions, i.e., purely factual uncertainty.

b. The risk of loss «from a contract that cannot be legally enforced» (Riskdimensions.com , glossary).

This example involves at least two norms. First, the contract must include at least one beneficial norm. Second, some other norm hinders enforcement and is thus detrimental to the stakeholder. The uncertainty with respect to the enforcement may be a normative uncertainty, but it could also be a factual uncertainty, or a combination of both.

c. Legal risk is the risk that the contract does not provide the level of protection intended by the contractors (Kredittilsynet 1994, section 2.4; similarly Norges Bank 1998).

5 The second part seems to build on the misconception that intellectual property rights can be «expropriated» by a trading partner. The term expropriation is usually used in other contexts. Possibly, the author meant to refer to a situation in which the intellectual property rights are acquired by a contract partner in a situation not controlled by the rights-holder. This may imply both legal and factual uncertainties.

This definition deals with a set of legal norms which is beneficial to the stakeholder, but where the degree of benefit is lower than intended. The definition does not address how this difference between intended protection and effective protection arises, e.g., whether the contract has not been sufficiently reviewed, was clearly misunderstood, or is simply interpreted differently than anticipated.

d. Legal risk: a change in the law «in a way that adversely affects a bank's position» (Wikipedia).

Many consider the change of law in example d) as a political, rather than a legal, risk. The uncertainty is somewhat hybrid. Admittedly, the uncertainty depends on the *fact*[6] that the lawmaker introduces changes, so it is mainly factual. However, frequent changes in law also may be said to have some impact on legal certainty, because they may make it more difficult to foresee the law's content. Indeed, many see the change of law as a separate type of legal risk (see below section 5.1).

e. «Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements» (Basel Committee on Banking Supervision 2006, footnote 97).

The Basel II definition focuses solely on legal norms which are detrimental to the stakeholder, i.e., as sources of risk. The definition does not address whether uncertainty related to this exposure has a factual or normative basis. Notably, legal risk is in this context understood as a type of operational risk. The latter term is defined similarly in Basel II and in the Banking Directive:

> *«Operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events, and includes legal risk» (Article 4 (22) of Directive 2006/48/EC).*

The Banking Directive does not define legal risk, so the banking sector is left with the Basel II definition. However, because the latter definition is explicitly non-comprehensive («includes, but is not limited to»), it recognizes the possibility that it omits a particular relevant type of legal risk, without providing any indication about what may have been omitted. As such, the definition provides little guidance about the core or the limits of the concept of legal risk.

6 The lawmaker's decision may again depend on a legal norm, such as an international treaty or a European directive.

It is therefore somewhat surprising that some important actors consider the Basel II definition a very useful definition. For example, the European Central Bank (2005/C 52/10) criticized that the draft of the Banking Directive did not define legal risk, and suggested that it «would be useful to introduce into the EU framework the more precise wording of Basel II.»

4.1.3 Descriptive conclusion

The semantic use and definitions of legal risk are inconsistent. Indeed, there seems to be no generally accepted definition of legal risk. Definitions and examples diverge with respect to three questions:

- Can there be a legal risk in the absence of any uncertainty? For example, can we speak of legal risk if the law is «not sound,» but is well-defined and predictable?
- Does legal risk encompass solely normative uncertainty, or does it also cover factual uncertainty? For example, should liability for an accident be included, if the only uncertain factor is whether or not the accident will happen?
- If we include factual uncertainty in relation to legal norms, where are the outer limits of legal risk? Should we include factually uncertain events which have consequences on an asset or objective for which the stakeholder holds some type of legal position? For example, should the breach of a contractual obligation by the other party be considered a legal risk?

These disagreements about the definition of legal risk build upon each other as illustrated in Figure 3. The following section addresses the questions raised here.

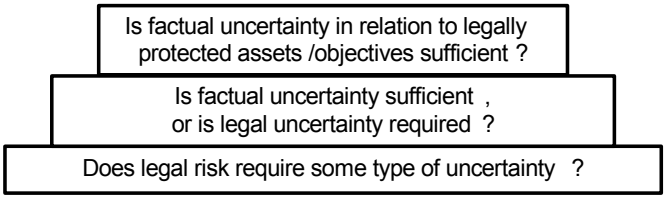


Figure 3 – Disagreements about legal risk

4.2 Prescriptive approach

The prescriptive approach applies the requirements to definitions mentioned above (Kolflaath 2004, pp. 79–92). First, a definition should clarify the meaning of the defined term in the relevant context. Second, a definition should provide a scope which is neither too wide nor too narrow. Third, the definition should facilitate and optimize decision-making based on it.

Regarding the first criterion, our context is quite wide and encompasses any form of legal risk management. The second requirement is most relevant in our context. We need to decide whether it is too narrow to define legal risk only in terms of legal uncertainty. Moreover, we need to determine whether it is too wide to include any uncertain event which has consequences for a normative position. With respect to the third requirement, decidability should be achieved by using terms which standardized approaches to risk management use and define.

4.2.1 An aspect of risk

It is probably not surprising that legal risk here is understood as an aspect of risk. This implies that there must be some type of uncertainty. Outside the scope of legal risk fall all definite or certain negative events, if there is no uncertainty. As a consequence, we cannot follow the above-mentioned UNIDROIT approach, which defines legal risk so widely that it covers even situations for which the law does not provide a *sound* solution, i.e., where the law does not fit the market reality. If the law is predictable but not sound, we lack the necessary uncertainty unless the facts are uncertain (which situation is addressed below). We thus require some type of uncertainty in any legal risk, and this uncertainty needs to be qualified.

4.2.2 Normative and factual uncertainties

The examples above reveal that there is no agreement with respect to whether the concept of legal risk is limited to legal uncertainty, or if the existence of factual uncertainty suffices.

When we speak of legal uncertainty, we typically assume a given set of facts and focus on the uncertainty regarding the correct or likely (Martin, Quinn et al. 2004; Ruger, Kim et al. 2004) legal judgement about these facts. This uncertainty is not related only to vague laws, but may arise from many different causes.

Bing 2006) has described a model to examine the causes of uncertainty in legal decisions. Apart from factual disagreements about the case's circumstances (where norms of evidence may also play a role), he mentions the following causes of uncertainty in legal decisions, as illustrated below in Figure 4.

- The variations of legal sources, which may be at hand for the decision maker. These variations may be related to availability or retrieval problems.
- Differences regarding the interpretation of the sources or understanding of the legal norms.
- The necessary uncertainty involved in norms leaving some margin of discretion to the decision maker.
- The decision maker's client or other loyalty, which makes certain interpretations more attractive than other possible alternatives.
- The law's overall certainty (where increased certainty often precludes the possibility of considering the case's unique nature).
- The «safety-valve» in law, which may allow the decision-maker to make adjustments in case the decision's consequences do not appear fair or reasonable according to extra-legal norms.

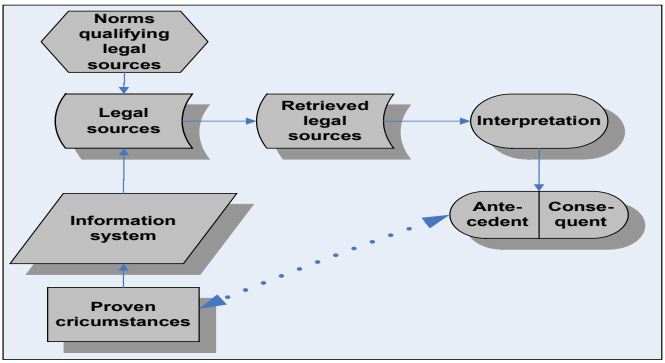


Figure 4 – Causes of uncertainty in a legal decision (Bing 2006)

Hence, the law's vagueness does not seem to be the only, and maybe not even the most important, source of legal uncertainty. Moreover, whether the law is necessarily vague is subject to a separate discussion. There are reasonable claims that law is necessarily vague (Endicott 2001; Endicott 2002) due to, among other factors, the problem that human behaviour is not foreseeable. For the purpose of this paper it suffices to state that the law's vagueness, in addition to other factors, permits different legal decisions, and that such decisions may lead to an unforeseen negative consequence for a stakeholder. Hence, legal uncertainty is indeed a very relevant source of legal risk. However, we need to ask whether legal uncertainty should be understood as *the only* source

of legal risk, or if a wider definition, which includes factual uncertainty, is more appropriate.

Factual uncertainties need to be considered in any type of planning for the future.[7] An example of factual uncertainty is that a stakeholder is the subject of a claim, e.g., based on an action for which he is liable. This type of risk is very frequently considered a legal risk, and is even the typical case of legal risk mentioned in the Basel II accord. It is essentially a question of pragmatics whether or not factual uncertainty should be included in legal risk. It may seem that legal uncertainty is the purest legal risk, because we can concentrate on legal methods to approach or calculate it. From the perspective of a stakeholder who analyses his risks, however, it may be difficult or impossible to distinguish the factual from the legal uncertainty, because the same risk may include elements of both types of uncertainty. Moreover, the wide use of the label «legal risk» sends a signal to the risk analyst or stakeholder, indicating that the risk analysis may require some research of legal aspects. Hence, this paper submits that the term «legal risk» should include both legal and factual uncertainties.

4.2.3 The outer limits of legal risk

The next open question regards the outer limits of the concept of legal risk. In principle, there seem to be two basic settings in which legal norms can play a role in risk. *First*, a legal norm may contribute to a loss for a stakeholder. In this case, the legal norm is one of the sources of the risk, and the legal risk has a legal norm as the *source of the risk*. The *second* setting is less obvious. A legal norm, in particular, a right or legal position, may play a role in protecting a certain asset or interest. An example of a legally protected asset would be an intellectual property right. In this case, the stakeholder is a rights-holder. Sometimes the literature uses the term legal risk (e.g., Hill 2005, glossary) in relation to possible events that will affect an *asset to which the stakeholder has a legal right*.

Example a) above defines legal risk very widely to include factual uncertainty with respect to assets (intellectual property rights) or objectives (protected in contract) for which the stakeholder holds a legal position. The problem with this wide understanding is that the world is full of assets and objectives for which there are legal positions, so it would be too wide to include in legal risk any factual uncertainties which affect a legally protected asset or interest. Moreover, the connotation of the term legal risk seems to imply that the risk somehow comes from the law, which is not the case here. The law merely

7 Moreover, factual uncertainties are the origin of a number of legal problems; see, e.g., Petersen, Henrichsen et al. 2005.

protects the stakeholder, and poses no risk at all. Hence, this wide understanding should be rejected.[8]

Thus, the term legal risk should be used in a more limited way. The concept «*source*» may facilitate a more restrictive definition. The ISO defines a source as an item or activity which has a potential for a consequence (ISO 2002, definition 3.1.5). In safety-related risk management, source is a hazard (ibid). Concomitantly, the concept of legal risk can be restricted in the intended manner by requiring that the term can be used only for risks which *include a legal norm as one of their sources*. This has two implications. First, it must be possible for the norm to be applied in a manner detrimental to the stakeholder. Second, the norm's existence and validity impact the risk value.

In summary, risk is the combination of the probability of an event and its consequences. A risk is a legal risk if its source involves a legal norm. Thus, the risk needs to be the manifestation of a legal norm's potential detriment. Both factual and legal uncertainty may influence legal risk.

5 Typologies of legal risk

The second question in this paper is whether we can identify meaningful types of legal risk. As mentioned above, we are particularly interested in the properties of exclusivity and exhaustiveness of the types of legal risk.

A possible categorisation could, of course, be based on the distinction between legal and factual uncertainty.[9] This duality would be an exhaustive enumeration,[10] but does not consist of mutually exclusive types, because any single risk may involve both legal and factual uncertainties. As section 5.2.3 below shows, however, it is possible to combine this distinction with other typologies.

5.1 Evaluation of existing approaches

The literature has suggested a number of typologies of legal risk, or sources of legal risk. All of the following typologies were proposed in the context of the financial market.

8 This does not, however, mean that legal risk management cannot or should not address such situations. The existence of a normative position indicates that the law may offer some kind of treatment to mitigate the risk. Hence, it is indeed useful to consider such situations under the label «risks which may be treated by legal means.»

9 Possibly the hybrid political risk of changing laws could be counted as a separate group. However, for the purpose of this paper we consider political risk as a type of factual risk.

10 This is true, at least if we categorize the somewhat hybrid political risk of changing laws as belonging to factual uncertainty.

5.1.1 Nydrén

Nydrén has suggested a classification of legal risk with respect to securitisation[11] (Nydrén 1995). Nydrén distinguishes documentation-related risk, legal uncertainty and changes in the law. Political risk (related to changes in the law) and legal uncertainty are discussed above. From this paper's perspective, the third category would have been expected to include all types of factual uncertainties. However, Nydrén's concept of «documentation-related» risk is much more limited; he defines it as «the risk that one communicates <B> but wanted to regulate <A>.» Nydrén seems to limit legal uncertainty to all norms outside the contract, which he denominates as «documentation.» This documentation-related risk seems to be a combination of contractual (legal) uncertainty and factual uncertainty. In this interpretation, this typology thus appears as a variation of the above-mentioned duality of legal and factual uncertainty.

5.1.2 Financial Law Panel

A paper by the English Financial Law Panel proposes three types of legal risks (Financial Law Panel 2001, see further McCormick 2006, pp. 108–109). These are (i) organisational legal risk, comprising risk related to the maintenance of a company's assets; (ii) legal methodology risk, relating to the possible utilization of inadequate methods to protect assets against claims or liability and (iii) conduct-of-business legal risk, which comprises obligations greater than foreseen and rights being more limited than expected. The first two groups, (i) and (ii), focus on deficiencies in assets' legal protection, and the third is based on a legal norm as a source of a risk. The types of legal risk described here seem to be non-exclusive. A risk related to the maintenance of a company's assets may be posed by insufficient protective methods, and may even be characterized as pertaining to the «conduct of business.» The typology seems to point to different aspects as criteria for differentiation, referring (i) to the protection of assets, (ii) to the methods employed for protection and (iii) to how the business is conducted. These criteria are so weakly defined that they cannot be understood as exhaustive.

5.1.3 International Bar Association working party

McCormick provided a quite different typology of legal risks in his function as chair of an International Bar Association (IBA) working party on legal risk

11 Securitization is a financial technique that pools assets and, in effect, turns them into a tradable security (Wikipedia). Notably, the term asset refers here to financial assets, which may imply that the term has a different meaning from the concept of asset mentioned above, which stems from security risk analysis.

(McCormick 2004). He mentions four causes of legal risk in the context of the financial market:

- «A defective transaction. Examples thereof include that the transaction does not allocate rights and obligations as intended, is void, is entered into on the basis of misleading representations, involves misunderstanding of its effects, lacks dispute resolution, etc.
- A claim or event which results in liability for the institution or other loss.
- Failure to protect assets (e.g., intellectual property).
- Change in law.»

In terms of exclusivity of the types of risk, there seems to be significantly less overlap between these types than in the above FLP typology. The defective transaction and the failure to protect assets are somewhat similar, at least if the «protection of assets» is understood widely. In a wide interpretation, the protections of assets could also encompass the protection of assets in transactions. Nevertheless, we have to suppose that the authors of this typology utilized a much narrower definition of asset, thereby achieving exclusivity.

The International Bar Association working party did not address whether these types are meant to be exhaustive. Because the typology was proposed in the context of the financial market, the working party has presumably left open the possibility that this typology of legal risk would need to be adapted to other sectors. Indeed, the term «transaction» may be less relevant in a different context than it is here. For example, if we assume a situation in which an employee's risk is assumed to be the possibility of his employment contract being invalid, this is not related to a «transaction.» But even in the context of the financial market, it may be possible to think of additional types not covered here. For example, the second bullet point does not explicitly address whether criminal liability is included. Moreover, it mentions only «liability for the institution,» and not liability for the institution's directors or other personnel. Thus, there are indications that this typology cannot be understood to be exhaustive. Nevertheless, the latter typology is probably quite useful as a starting point for discussion from the context of the financial markets, not least due to its clear wording and concreteness.

5.1.4 McCormick: Type 1 and Type 2 risks

McCormick 2006, p. 10) describes legal risk as follows (emphasis added):

> *«Legal risk is a particular kind of risk. It is commonly understood to relate to the risk of being sued or being the subject of a claim or proceedings due*

> *to some infringement of laws or regulations, or the commission of a tort such as negligence or some other act giving rise to civil liability (referred to as 'Type 1 risks' in this book). However, in the context of the financial markets, the phrase is also frequently used to mean the risk of technical defects in the manner in which a transaction is carried out, resulting in loss, sometimes very serious financial loss, for those that put money at risk in the transaction. (We shall call that kind of risk a 'Type 2 risk'.)»*

This approach suggests a typology of risks simply by systematizing examples, without actually describing the difference between the two suggested types. Even the naming of the types is cryptic and fails to point out their key differences. Despite these shortcomings, McCormick's approach has some key advantages. Understood within the necessary norm-theoretical context, these types of legal risks may be understood to be *exhaustive* and, under certain conditions, *exclusive*, which is shown below (section 5.2.3). Both types of risks may be interpreted to focus clearly on *legal norms as sources of risk*, which is in line with our definition. Type 1 risks' source includes a norm which holds the grounds for being sued, exposed to liability, etc. Type 2 risks' source includes a norm which determines that the transaction has «technical defects,» as McCormick puts it.

However, we have not yet addressed the key point. What is the essential difference between type 1 and type 2 risks? In order to answer this question, we first need to take a closer look at norm theory.

5.2 Norm theoretic typology

Our starting point is that the *concept* of legal norm is not constructed, but is a reflection of an existing phenomenon.[12] The legal system forms a «scheme of interpretation» (Kelsen 1960, pp. 3–4) to judge facts. The norm theory presented here seeks to clarify and understand the *micro perspective* of this scheme of interpretation. In this micro perspective, the legal norm is the key concept which steers the interpretation of facts. Norm theory suggests that we can distinguish at least two types of legal norms, which here are named *deontic* norms and *qualification* norms.

12 Of course, this does not prevent the existence of different opinions about what constitutes a legal norm.

5.2.1 Deontic norms

A deontic norm prescribes what is obligatory, prohibited or permitted for an actor.[13] Deontic norms are sometimes referred to as «duty-imposing norms» or «prescriptive norms,» but here we use the term «deontic norm,» which forms the basis of deontic logic (von Wright 1951). Legal systems offer a set of possibilities to enforce deontic norms.

5.2.2 Qualification norms

In addition to deontic norms are other norms, which do not impose an obligation, prohibition or permission. We call these norms qualification norms, because they *qualify* a set of facts as something which has a legal meaning. This is often expressed by saying that «x shall count as y» (Eckhoff and Sundby 1988, p. 86). Qualification norm is a term used by, e.g., Eckhoff and Sundby 1988, p. 78), but the same concept is referred to as a constitutive norm (Herrestad 1996, p. 142), as secondary norm by Hart 1994 (p. 94) or as determinative rule by von Wright 1963 pp. 6–7). The concept of a qualification norm may be understood more easily by reference to examples.

These examples are introduced with respect to the two major types of qualification norms, i.e., *competence* and *validity*. For example, with respect to a contract, there are a number of validity norms. Such norms may, e.g., state that a certain type of contract, say, a real estate contract, is valid only if it is concluded in writing. This norm qualifies a particular set of facts as something which has a specific legal meaning, namely, a valid real estate contract. The second relevant type of qualification norm regards competence, i.e., *who* has the competence or power to do *what*. Competence norms are sometimes referred to as power-conferring norms (Bulygin 1992), and the competence may relate to public or private matters. Competence norms are made explicit, e.g., in constitutional law, in statements such as, «The Bundestag decides about the laws of the Federal Republic of Germany» (Article 77 of the German Constitution). Lack of competence should not be confused with prohibition; no one is prohibited from issuing a federal law for Germany, but such an act would lack validity. However, it is not always the case that lack of competence leads to invalidity. For example, if the highest court in a system issues a judgment which is outside its competence, there may be no court left to which to make an invalidity claim (Eckhoff and Sundby 1988, p. 83). Notably, competency norms are sometimes considered a separate type of norms (Eckhoff and

13 Sometimes, this is complemented by a fourth type of deontic norm, relating to acts which are not obligatory; see Eckhoff and Sundby 1988, p. 66. This distinction is not necessary in our context.

Sundby 1988). However, for the purpose of this paper we simplify the picture and consider competency norms as a type of qualification norms.

5.2.3 A norm-theoretic approach to legal risk

A norm-theoretic approach should take as its starting point that legal risk is a risk that has a deontic or qualification norm as its source.

An example of a *deontic norm as the source of a risk* would be the above mentioned Type 1 legal risk described by McCormick 2006):

> *«the risk of being sued or being the subject of a claim or proceedings due to some infringement of laws or regulations, or the commission of a tort such as negligence or some other act giving rise to civil liability.»*

The possibility of being sued is perceived as a risk primarily because it may end with a judgment which *obliges* the stakeholder to perform a particular action, or which *prohibits* him from performing an action he considers beneficial. A deontic legal risk is thus related to an event influenced by a deontic norm.

A *qualification norm as the source of a risk* is included in McCormick's example of a Type 2 risk:

> *«[…] technical defects in the manner in which a transaction is carried out, resulting in loss, sometimes very serious financial loss, for those that put money at risk in the transaction.»*

The technical defects in this example are bound to be related to qualification norms, in particular, those dealing with competence and validity. According to McCormick, the landmark case for legal risk in the financial market in London was *Hazell v Hammersmith and Fulham London Borough Council* ([1992] 2 AC 1), in which the House of Lords decided that the city council had no power enter into a certain type of financial transaction. The consequence of this lack of competency was a financial loss on the part of the bank. It may, of course, be confusing that this financial loss again materializes through a deontic norm, e.g., making it not obligatory for the city council to pay back a certain amount of money. However, the latter deontic norm is not the root of the uncertainty in this case. The root of the uncertainty was the city council's (unexpected) lack of competency.

This distinction between deontic and qualification norms fulfils the requirements of exclusivity set out above, provided that we can single out one norm as the single source of risk. As soon as there is uncertainty about two or more norms, the types are no longer exclusive. However, if one norm can be singled

out as the only uncertain one, then it is normally either dontic or qualificatory.[14] Nevertheless, it may not be trivial to decide whether the norm is a qualification or a deontic norm, as this may depend on the perspective.

This typology is exhaustive; this is to say that if all relevant deontic and qualification norms have been considered, every possible legal risk is covered. Regrettably, this is only of limited use in a practical perspective, because it does not indicate where or how these types of sources of legal risk can be identified. This risk identification needs to be done in a context-dependent approach, e.g., following the lines of one of the lists of legal risk analysed above in section 5.1. However, the practical use of the norm-theoretic approach is greatly improved if it is combined with the above-mentioned distinction between legal and factual uncertainty. This combination of approaches renders a matrix of legal risk as shown in Table 2. The table could even be expanded by adding additional levels for the sub-types of norms in each class.

	Legal uncertainty	**Factual uncertainty**
Deontic norm	**I may have to pay taxes** (depending on interpretation of tax law).	**I may have to pay damages** (depending on whether I cause an accident while driving and drinking).
Qualification norm	**The contract may not be valid** (depending on uncertain validity rules).	**The contract may not be enforceable** (depending on whether a claim is submitted within the time limitation).

Table 2 – Combination of this paper's perspectives on legal risk

6 Concluding remarks

This paper has reviewed a number of approaches to legal risk. The inconsistent use of the term legal risk in literature and practice leaves us with the impression that legal risk is little more than one of many perspectives on risk. Legal risk is often, at the same time, financial risk or political risk. Nevertheless, this discussion of legal risk in a prescriptive perspective indicates that it is possible and useful to point out the *differentiating criteria* legal risk should fulfil. *First,* the paper submits that legal risk should address and cover events which are

14 Notably, Eckhoff and Sundby 1988 (on p. 82) explicitly consider the possibility of one norm pertaining to more than one category.

uncertain, based on both factual and legal uncertainty. *Second*, reference to a legal norm is not sufficient if this norm is beneficial solely to the stakeholder. Hence, a legal norm in a risk can constitute a legal risk only *if the norm can be qualified as a source of risk*.

Once the definition of legal risk has been clarified, we are interested in understanding what *types of legal risk* there are. Many typologies suggested by practitioners are essentially context-dependent, non-exhaustive and do not consist of mutually exclusive types of legal risk. Hence, they may be very useful in their specific context, but they do not form a solid basis for a general theory of legal risk. Quite the opposite is the case for the norm-theoretic approach outlined above. The distinction between deontic and qualification norms as sources of legal risk enables us to clearly distinguish two types of legal risk, under the condition that we face a single relevant norm. The combination of the norm-theoretic approach with the distinction of normative and factual uncertainties renders a matrix of legal risk, which should be generally applicable for the identification of legal risks, independent of the context.

7 Acknowledgements

The research presented in this paper was funded by the Research Council of Norway through the project ENFORCE.

Norwegian Research Center for Computers and Law (NRCCL)
Faculty of Law
University of Oslo
P .O. Box 6706 St. Olav's plass
N-0130 Oslo
Norway

8 References

Bank of England (2000). Oversight of payment systems. Quoted by McCormick 2006, p. 107.

Basel Committee on Banking Supervision (2006). International Convergence of Capital Measurement and Capital Standards. A Revised Framework, Comprehensive Version. Bank for International Settlements.

Ben-Haim, Y. (2006). Info-gap decision theory: decisions under severe uncertainty. Amsterdam: Elsevier.

Bernstein, P. L. (1996). Against the gods the remarkable story of risk. New York: Wiley.

Bing, J. (2006). Trust and Legal Certainty in Electronic Commerce: An Essay. Festskrift till Peter Seipel. Stockholm: Norstedts Juridik AB: 27–49.

Bulygin, E. (1992). On norms of competence. Law and Philosophy 11(3): 201–216.

Burnett, R. (2005). Legal risk management for the IT industry. Computer Law & Security Report 21(1): 61–67.

COSO (2004). Enterprise risk management: integrated framework. Committee of Sponsoring Organizations of the Treadway Commission.

EADS (2005). Annual Report and Registration Document 2005: Financial Statements and Corporate Governance. Filed with the Dutch Market Authorities 2006.

Eckhoff, T. and N. K. Sundby (1988). Rechtssysteme: Eine systemtheoretische Einführung in die Rechtstheorie. Berlin: Duncker & Humblot.

Endicott, T. (2001). Vagueness in Law: Oxford Univ Press.

Endicott, T. (2002). LAW IS NECESSARILY VAGUE. Legal Theory 7(04): 379–385.

Eng, S. (2003). Analysis of dis/agreement with particular reference to law and legal theory. Dordrecht: Kluwer Academic Publishers.

Financial Law Panel. (2001, DRAFT 26/07/01). „LEGAL RISK ASSESSMENT.« from http://www.fmlc.org/papers/flp_050926c.pdf.

Hansson, S. O. (2005). Decision Theory-A brief introduction Stockholm: Department of Philosophy and the History of Technology, Royal Institute of Technology (KTH)

Hansson, S. O. (2007). Risk. Stanford Encyclopedia of Philosophy

Hart, H. L. A. (1994). The concept of law. Oxford: Clarendon Press.

Herrestad, H. H. (1996). Formal theories of rights. Oslo

Hill, C. W. L. (2005). International Business: Competing in the Global Marketplace: McGraw-Hill/Irwin.

ISO (2002). Risk management – vocabulary – guidelines for use in standards. Geneva: ISO.

Kelsen, H. H. (1960). Pure Theory of Law. London

Kenny, M. (2004/2005). Legal risk and the financier. Network and Correspondent Banking Review 22–24.

Keskitalo, P. (2000). 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. Helsinki: Kauppakaari.

Knight, F. H. (1921). Risk, uncertainty and profit. Boston: Houghton Mifflin.

Kolflaath, E. (2004). Språk og argumentasjon – med eksempler fra juss. Bergen: Fagbokforlaget.

Kredittilsynet (1994). Rundskriv 51/1994.

Luhmann, N. (1972). Rechtssoziologie. Reinbek bei Hamburg: Rowohlt.

Luhmann, N. (1993). Risk a sociological theory. Berlin: Wallter de Gruyter.

Mahler, T. and J. Bing (2006). 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.

Martin, A. D., K. M. Quinn, et al. (2004). Competing Approaches to Predicting Supreme Court Decision Making. Perspectives on Politics 2(04): 761–767.

Mas-Colell, A., M. D. Whinston, et al. (1995). Microeconomic theory. New York ; Oxford: Oxford University Press.

McCormick, R. (2004). „THE MANAGEMENT OF LEGAL RISK BY FINANCIAL INSTITUTIONS.« from http://www.federalreserve.gov/SECRS/2005/August/20050818/OP-1189/OP-1189_2_1.pdf.

McCormick, R. (2006). Legal risk in the financial markets. Oxford: Oxford University Press.

Norges Bank (1998). Petroleumsfondet: Årsrapport 1998.

Nydrén, B. (1995). Om kreditrisker och juridiska risker vid s.k. värdepapperisering. Svensk Juristtidning: 221–240.

Petersen, H., C. Henrichsen, et al. (2005). Ret og usikkerhed. København: Jurist- og Økonomforbundets Forlag.

Riskdimensions.com. «Glossary.» Retrieved 30 Nov. 06, from www.riskdimensions.com/resources/glossary/, text removed and only available through google.com.

riskdimensions.com. «Glossary. Legal risk.» 2006, now withdrawn, from www.riskdimensions.com/resources/glossary/.

Ruger, T. W., P. T. Kim, et al. (2004). The Supreme Court Forecasting Project: Legal and political science approaches to predicting Supreme Court decisionmaking. Columbia Law Review 104(4): 1150–1209.

Sandvik, T. (1966). Entreprenørrisikoen. Oslo: Tanum.

Selvig, E. (1965–1978). The freight risk. Arkiv for sjørett 7: 1–512.

Smith, R. (2006 (Winter Edition)). Aristotle's Logic. The Stanford Encyclopedia of Philosophy. E. N. Zalta.

Steele, J. (2004). Risks and legal theory. Oxford: Hart.

Trzaskowski, J. (2005a). Legal risk management -- some reflections. Julebogen 2005: DJØF Publishing: 175–180.

Trzaskowski, J. (2005b). Legal risk management in electronic commerce managing the risk of cross-border law enforcement. København: Ex Tuto.

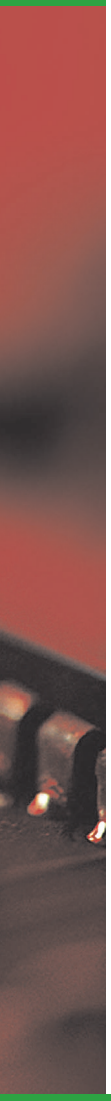
von Wright, G. H. (1951). Deontic Logic. Mind 60(237): 1–15.

von Wright, G. H. (1963). Norm and action: a logical enquiry. London: Routledge & Kegan Paul.

Wahlgren, P. (2003). Juridisk riskanalys: mot en säkrare juridisk metod. Stockholm: Jure.

Wikipedia. (30 March 2007). «Legal Risk.» from http://en.wikipedia.org/wiki/Legal_risk.

Wittgenstein, L. (1997). Philosophische Untersuchungen. Oxford: Blackwell.



Hvert år oppfordrer vi våre forskere til å gi bort en artikkel til jul. Dette er syvende 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 seventh 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.

- Fremtiden på spill
- I strafferettens tjeneste
- Organisasjonsendring i sivilsamfunnet. Teknologisk endring og nye rettslige krav.
- Making Sense of Digital Cash
- Møte mellom forvaltningsretten og personopplysningsretten
- Fra skatt ved hullkort til studielån via SMS
- Identity Management and Data Protection Law
- Kunnskap som vernet gode – et essay
- Knowledge Economy theories underpinning EU's i2010 strategy and their (in)capacity for representation in a regulatory framework for Nigeria
- Defining legal risk

ISBN 978-82-7226-107-7