Høgskolen i Hedmark

Olav Nyhus

Masteroppgave

Personvern – konfidensialitet

Instrumentelt eller institusjonelt fokus?

Privacy - confidentiality

MPA 7

2014

Samtykker til utlån hos høgskolebiblioteket JA ☒ NEI ☐

Samtykker til tilgjengeliggjøring i digitalt arkiv Brage JA ☒ NEI ☐

Innhold

1. Forord

Etter at jeg ble cand. jur. våren 1994, har jeg hele tiden arbeidet i ulike offentlige organisasjoner. Alle har i større eller mindre grad hatt høyt fokus på sine brukere. I mine knapt 14 år i Forbrukerrådet var forbrukerperspektivet bærende for all virksomhet i organisasjonen. Dette har preget min yrkesmessige tilnærming til oppgavene jeg har blitt tillagt.

I 2010 ble jeg ansatt som rådgiver for internkontroll i den organisasjonen jeg er nå. Ansvaret for informasjonssikkerheten er i vår organisasjon sett på som en del av internkontrollen. Både arbeidsgiver og jeg var nok noe famlende i arbeidet med å definere både rollen og funksjonen. Det er noe av bakgrunnen for at jeg høsten 2011 startet på Master of Public Administation ved høyskolen på Rena. Studiet har tilført meg mye ny og nyttig kunnskap om offentlig virksomhet.

Jeg har i mange år vært spørrende til om det er en optimal måte vi styrer organisasjoner, og også om måten vi styrer medarbeiderne i organisasjoner. Bakgrunnen for undringen er bruken av økonomiske styringssignaler som en del av budsjett prosessen. Særlig at målformuleringen og kravene til rapporteringen er angitt i tallstørrelser for verdier eller mål som ikke lar seg tallfeste, er egnet til å undres over.

Min arbeidssituasjon endret seg i forbindelse med permisjoner og sykdom hos kollegaer. Det innebar at jeg fikk et overordnet ansvar for Kommunal oppreisningsordning i Østfold. Senere også et daglig driftsansvar som fungerende sekretariatsleder. Denne ordningen ga tidligere barnevernsbarn mulighet for å søke om oppreisning for den urett som ble begått mot dem mens de var under offentlig omsorg. Det ligger i sakens natur at dette omfattet forvaltning av mye personsensitivt materiale.

Siden informasjonssikkerhet er definert som en del av internkontrollen har jeg deltatt på flere kurs og konferanser om dette temaet. Det har lært meg at utfordringene er store, og det er vannskelig å holde tritt med de stadig nye utfordringene i den digitale utviklingen. Dette gjelder både internt og i forholdet til utstyrs leverandører, og i forhold til brukere. En særlig utfordring er at de som benytter digitalt nettverk for å snoke, eller til kriminell aktivitet, ofte vil ligge i fokant.

I forlengelsen av dette var valget informasjonssikkerhet som tema for min masteroppgave nærliggende. Temaet måtte avgenses for å bli hånderbart innenfor et slikt format. Derfor er

det personvern som er temaet, men dette temaet er kanskje endra større uten en presisering av hva det betyr i kontekst med informasjonssikkerhet. Det er etter dette kravet om å holde personopplysninger hemmelig, med unntak av de tilfellene det er lovlig tilgang, som er hovedfokuset. Drøftelsen er delvis styrt av min interesse for styringsperspektivet. Oppgaven handler derfor om hvorvidt årsaken til hvor godt eller dårlig vi lykkes med hemmelighold av personopplynsinger, ligger i styringen.

Jeg vil gjerne takke alle lærerne og medstudentene som har bidratt på MPA 7. Det har for meg vært både spennende, utfordrende og endrende. En spesiell takk til min veileder Sjur Kasa som har gitt meg raske og gode tilbakemeldinger underveis. Bibliotekeket på Høyskolen i Hedmark, både på Rena og ellers, skal ha honnør for servis-instilling og raske ekspederinger av enhver forespørsel. Takk også til mine informanter, - uten dem hadde det ikke vært noe empirisk grunnlag å drøfte.

Takk til venner, kollegaer og medstudenter for interesse og støtte. En takk også til min arbeidsgiver som har gitt meg mulighet for denne videreutdannelsen både i form av tid og kostnadsdekning. Sist, men ikke minst vil jeg takke familien min som har støttet meg og akseptert min manglende tilstedeværelse i flere sammenhenger. Særlig min kone Mette fortjener stor takk for støtte, anerkjennelse og gode samtaler.

2. Innledning

«Når skjønner vi at personvernet bare er en illusjon og at husets fire vegger ikke lenger er der?» spør *Mathilde Fasting* i et innlegg i Minerva 03.02.14 (Fasting, 2014). Innlegget er skrevet i relasjon til innføring av smarte strømmålere med to-veis kommunikasjon i alle norske husstander. Konsekvensen er at strømforbruket blir registrert time for time. Dette vil avsløre mye om de som bor der. F.eks. når de er hjemme, hvor mange som bor der, om de benytter strøm til oppvarming m.m. Dette er personopplysninger som, eventuelt koblet med annen informasjon, vil kunne ha en markedsverdi. Opplysningene vil også ha en «verdi» for eksempelvis innbruddstyver.

Det kan være grunn for reflektere over om Fastings spørsmålet er mer allment. Det synes som det er konfidensialitetsperspektivet i personvernet som er Fastings bekymring. Det er vel også den betydningen som legges i begrepet «personvern» i alminnelig tale. Det som gjerne omtales som «privatlivets fred». Begrepene «personvern» og «informasjonssikkehet» brukes gjerne litt om hverandre, og har en nær beslektet betydning. Jeg skal nedenfor redegjøre for både disse og andre sentrale begrep.

2.1 Presentasjon

Jeg skal her redgjøre for temaet for denne oppgaven, og presentere problemstillingen som reises.

Det overorndnede temaet er personvern. Dette har et stort omfang, og er relatert til flere perspektiver. Mye av det som er forsket og teoretisert over tidligere handler om tilfeller der personvernet blir utfordret av andre verdier som også vurderes som viktige. Eksempler kan være:

1. Personvern og forholdet til ytringsfriheten. Her kan det reises spørsmål om foreldres publisering av personopplysninger om egne barn og barnas personvern. Presse-etiske dilemmaer er sentralt. Aktuelle spørsmål her kan være omtale av selvmord og selvmordsforsøk, identifisering av personer i staffesaker m.v.
2. Personvern og sammfunnssikkerhet. Her er spørsmålet om f.eks. forsvarets og Politiets sikkerhetstjenestes innsamling av personopplysninger kan begrunnes ut fra hensynet til rikets sikkerhet. Dette perspektivet har også fått en internasjonal dimensjon etter at

det ble avdekket at bl.a. USA samler inne slik informasjon ikke bare om egne borgere, og ikke bare av hensyn til egen sikkerhet.

3. Personvern og arbeidsgivers styringsrett. Her vil problemstillingen være hvorvidt arbeidsgiver kan benytte personopplysninger som er samlet inn for et formål, også kan benyttes til andre formål. Høyesterett behandlet en anke i en sak hvor det var krav om overtidsbetaling og hvor arbeidsgiver la fram en GPS utskrift som viste arbeidstakers bevegelser. Selv om innsamlingen av GPS bevegelser hadde som formål å effektivisere driften, ble den tillatt fremlag for et annet formål. (Høyesteretts ankeutvalgs kjennelse, 19.05.2011, HR-2011-01019-U, (sak nr. 2011/787), sivil sak, anke over kjennelse.)

Disse eksemplene gir ikke noe fullstendig bilde på ufordringer med kryssende interesser, men gir en indikasjon på omfanget.

Jeg skal nevne to eksempler hvor personvernet også blir utfordret av misbruk, eller forsøk på misbruk. Her er det kriminell virksomhet eller innsamling av personopplysninger som har en økonomisk verdi i f.eks. markedsføringsøyemed som jeg tenker på. Det er stadig saker i media som viser en del av de utfordringene som ulike organisasjoner sliter med. Dette gjelder både private og offentlige virksomheter. Det er særlig to forhold som har vært på medienes agenda. Det ene er knyttet til den enkeltes økonomiske verdier. Eksempler her er innlogging i nettbanker hvor enten bankenes systemer blir utfordret, eller hvor kundenes innloggingsinformasjon blir stjålet. I samme kategori er de tilfellene hvor bank-/kreditkort blir stjålet/kopiert sammen med kode eller annen brukeridentifikasjon. Dette er også et angrep på personvernet selv om det økonomiske angrepet naturlig nok får størst oppmerksomhet.

Det andre forholdet jeg vil nevne er der individers personlige opplysninger kommer på avveie. Dette kan skje både frivillig og ufrivillig. Det siste er åpenbart tilfelle der opplysninger hos det offentlige om et klientforhold lekker ut. Enten det er tilknytning til barnevern, NAV eller helseopplysninger, er det selvsagt uakseptabelt. I andre tilleller gir vi fra oss opplysninger om et kundeforhold helt frivillig, eller uten at vi vet det. I noen tilfeller mot noen fordeler, men også noen ganger av ren bekvemmelighet. Disse opplysningene kan systematiseres og selges siden de har en verdi for andre selskaper i en markedskommunikasjon. Mange vil tenke at det er fint at markedsføringen er tilpasset meg og mine preferanser. Grensen mot det ubehagelige private vil være ulik, men tilbud om å kjøpe bleier 9 måneder etter at du sluttet å kjøpe sanitetsbind, er for mange for privat. Tilsvarende påtrengende vil mange oppleve det ved spesialtilpassede tilbud på produkter i kategorien apotekervarer.

Disse eksemplene viser at personvern er et stort og mangefasettert tema. Jeg har pekt på noen utfordringer som personvernet møter, men hva ligger egentlig i begrepet? Rent språklig kan vi si at det handler om vern av person. En slik tilnærming kan indikere alt fra sikkerhetsutstyr for fysisk beskyttelse, til å verne barn mot deler av virkeligheten de ikke er modne for å fordøye. Personvern i denne oppgaven har en annen betydning, og det skal klargjøres i det følgende.

Hva er personvern?

Personvern er definert en rekke steder. Her skal nevnes noen av de sentrale definisjonene.

1. Menneskerettigheter (Den europeiske menneskerettskonvensjon)

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

2. Grunnloven

§ 102.
Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.
Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet.

3. Regjeringen

Personvern kan defineres og beskrives på ulike måter. Sentralt står imidlertid det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred. Personvernet er derfor nært knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse. Retten til privatliv følger bl.a. av den europeiske menneskerettskonvensjon (EMK) artikkel 8 og står sentralt i EUs personverndirektiv (95/46 EF). Disse internasjonale regelsettene ligger til grunn for vår nasjonale personvernlovgivning. (regjeringen, 2014)

4. Datatilsynet

Enkelt sagt handler personvern om retten til et privatliv og retten til å bestemme over egne personopplysninger. (Datatilsynet, 2014)

5. Personopplysningsloven

> *§ 1.Lovens formål*
> *Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.*
>
> *Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.*

Som man ser av disse sentrale formuleringene er det hensynet til den enkeltes personvern og individets rettigheter som står sentralt.

Dette viser tydelig at temaet personvern må **avgrenses** for å bli hånderbart innenfor formatet til denne oppgaven. Som tittelen indikerer vil jeg avgrense til konfidensialitet. "Konfidensielt" er nesten synonymt med "hemmelig". Innenfor temaet personvern regnes konfidensialitet også som et prinsipp om at personopplysninger skal være sikret mot at uvedkommende får tilgang til dem. (Datatilsynet, 2014)

Videre vil jeg avgrense til offentlige organisasjoner. Årsaken til det er at oppgaven har en statsvitenskaplig tilnærming, og særlig mot styring av offentlige organisasjoner. Styringsperspektivet eller måten man styrer på, er sentralt i forhold til krav om å nå de ulike målene som er satt. Dette gjelder selvsagt enten det er nasjonale mål eller i den enkelte organisasjon.

I denne sammenhengen er målet i utgangspunktet noe difust. Det følger av både rettsregler og av en alminnelig oppfatning at enhver har krav respekt for sitt personvern. Det innebærer at når offentlige organisasjoner samler inn og forvalter personlige opplysninger, må behandlingen være forsvarlig for å sikre det enkelte individs krav på personvern. Ansvaret i organisasjonen må alltid ledelsen bære. Det betyr i alminnelighet at det gis noen styringssignaler som forventes å gi det ønskede resultat.

Offentlig sektor har noen felles nasjonale forpliktelser å ivateta. Det betyr at staten eller regjeringen vil måtte stå til ansvar for manglende måloppnåelse både på nasjonalt og også

eventuelt på internasjonalt nivå. Dette vil i alminnelighet føre til at det gis overordnede styringssignaler. Det er ulike dimensjoner ved styring, og det kan komme til utrykk både ved politiske signaler, finansiering eller økonomistyring, andre insentiver eller kontroller og sanksjoner. På personvernområdet har styringen kommet til uttrykk bl.a. i form av lovregulering, oppdragsbrev og politiske ytringer. Slike nasjonale føringer er gitt for å sikre enkeltmenneskets krav på personvern.

Styringen for å fovalte personvernet har derfor flere ledd, eller flere nivåer om man vil. Den statlige styringen vil eventuelt via fagmyndighet nå det enkelte organisasjonsnivå. Derfra vil styringssignalene treffe den enkelte organisasjon og til slutt den enkelte medarbeider. Underveis vil styringssignalene tolkes og operasjonaliseres med ulikt detaljnivå. Når det gjelder personvernet konkret er de overordnede reglene om personvern i blant annet Grunnloven blitt operasjonalisert til å være en del av informasjonssikkerheten i personopplysningsloven. Krav om informasonssikkerhet er den enkelte organisasjon pålagt. Selve begrepet "informasjonssikkerhet" skal jeg komme tilbake til en definisjon av senere. Poenget her er at personvernet den enkelte har krav på er operasjonalisert, eller oversatt, til et krav til organisasjonene.

Vi vet at informasjonssikkerheten, og derved personvernet, ikke er tilfredstillende ivartetatt. Se senest Riksrevisjonens årsrapport for 2013 (Riksrevisjonen, 2014). Forskningsspørsmålet som jeg vil søke å belyse er derfor:

Hvorfor har vi ikke et godt personvern i offentlige organisasjoner?

Det kan være flere årsaker til dårlig måloppnåelse på dette temaet. En overordnet forklaring kan være at reglene ikke følges, og årsaken til det kan være manglende prioritering eller insentiver som ikke fungerer. En annen forklaring kan være at reglene og den overordnede styringsformen ikke er egnet for å nå målet. Begge disse forklaringene er relatert til styringssignalene og styringen av organisasjoner og medarbeidere. Det er derfor interessant å forske på styringen for se om det kan finnes forklaringer til manglende måloppnåelse der.

Problemstillingen jeg reiser er følgelig:

Ligger årsaken til dårlig personvern i offentlige organisasjoner i styringen?

Allerede overskriften for oppgaven indikerer at min hypotese er forankret i hvilken innretningen styringen har.

Særlig er jeg interessert i om det er en sammenheng mellom hvordan organisasjonen er styrt, og hvilket verdigrunnlag som den bygger på, og etterlevelsen av konfidensialiteten. Det er i statlig sektor nærmest et generelt påbud om å benytte en mål- og resultatstyring (Senter for statlig økonomistyring, 2014), og et tilsvarende styringssett er også vanlig i kommunene. På kommunalt nivå kommer dette som en naturlig følge av de statlige rapporteringskravene på enkelte områder, og kan ofte utvikle seg til en generell praksis. Den økomiske styringen som normalt har et slikt preg, vil også kunne være en del av forklaringen. En slik tilnærming vil være preget av instrumentelle virkemidler, og hvor resultatoppnåelsen i alminnelighet skal rapporteres i en tallstørrelse. Alternativet er en verdibasert styring ved at verdien som skal søkes oppnådd blir presentert verbalt, og at det følger med en slump penger i håp om at verdien skal oppnås ved tjenesteproduksjonen eller hva det måtte være det skal gis styringssignaler i forhold til. For meg er det opplagt at det her som ellers ikke kan være noe enten/eller, men et både/og. Det kan være grunn for å reflektere over om styringssystemet fungerer godt for å løse alle typer oppgaver. Er det særlig er rapporteringskravene, og koblingen til indikatorer ikke er dekkende, eller er det styringen som sådan?

Det er ulike resultatmål eller verdier som skal oppnås i en offentlig organisasjon. På den ene side er det klare produksjonsmål som skal oppnås med hensyn til både kvantitet og kvalitet. På den andre side er det krav om at organisasjonen til enhver tid f.eks. skal foreta en etterrettelig saksbehandling, at demokratiperspektivet, herunder offentlighet, blir ivaretatt, og at både ansatte og brukere sikres personvern. (Se om dette bl.a. i forvaltningsmeldingen (St.meld.nr 19, 2008-2009, pkt 3.4 og 3.5) (Regjeringen, 2014) med en omtale av fire grunnleggende verdier som skal ligge til grunn for statsforvaltningens virksomhet.) Disse eksemplene på andre løpende krav til organisasjonen vil man kunne tone ned uten at det får konsekvenser. Men dersom det avdekkes manglende ivaretakelse, vil det ofte være utfordrende for omdømmet. Manglende, eller svak, internkontroll er uten betydning før «noe» skjer eller det blir foretatt ett tilsyn.

Og her er vi ved sakens kjerne i forhold til styring og kontroll: et tilsyn vil avdekke mangler på systemer, regler, rapporteringer og avvik. Men når avvikene er lukket og reglene på plass, er da verdiene demokrati, offentlighet og personvern blitt en del av verdiene som ivaretas i organisasjonen? Eller er situasjonen like nedslående ved neste tilsyn? Riksrevisjonens rapport for 2013 (Riksrevisjonen, 2014) peker på at det er flere gjengangere som har samme utfordringer som tidligere, og/eller som ikke har fulgt anbefalingene Riksrevisjonen kom med

forrige gang. Det indikerer at situasjonen i hvert fall i noen tilfeller er like nedslående ved neste tilsyn.

Problemstillingen er i ytterste konsekvens om statens styringssystem, og herunder etablering av tilsynsinstanser, er egnet til å generere slike verdier som er formulert.

Min hypotese er forankret i institusjonell teori (dette behandles nedenfor), og en forestilling om at verdibasert implementering av personvern vil fungere bedre enn bare å innføre regler og systemer.

Hypotesen kan da formulers slik:

> ***En større grad av institusjonell tilnærming gir bedre personvern***

2.2 Bakgrunn

Hvorfor er det interessant å forsøke å identifisere årsaker til manglende personvern i offentlige organisasjoner? Det åpenbare utgangspunktet er at personvernet er dårlig ivatetatt. På statlig nivå er prioriteringen i følge Riksevisjonen ikke tilstrekkelig (Riksrevisjonen, 2014). De uttaler i forbindelse med publisering av rapporten:

> *Riksrevisjonen viser til det ansvaret som Kommunal- og moderniseringsdepartementet (tidligere Fornyings-, administrasjons- og kirkedepartementet) har for en styrket og mer helhetlig ikt-sikkerhet i statsforvaltningen. Det ble påpekt allerede i 2009 at flere slike samordningsoppgaver ikke var gjennomført. Til tross for økt avhengighet av ikt, endret risikobilde og økt satsing på ikt-systemer, har departementet fortsatt ikke ferdig en plan for arbeidet med informasjonssikkerhet.*

Når det settes fokus på personvernet synes svaret på utfordringene å være mer av det samme. Se f.eks. Stortingsmelding nr 11 (2012-2013) «Personvern – utsikter og utfordringer» (Regjeringen, 2014) hvor konklusjonen er at «personvernstyremakta i hovedsaka fungerer tilfredsstillande». Videre uttales det at personvernrådgivere og en sterk lederforankring kan ha en positiv effekt. Det vil derfor vurders endringer i ordningen med personvernombud. Noen refleksjon om muligheter for endring i styringssignaler, synes fraværende. Det er i hovedsak virkemidlene det reflekteres over.

Tidligere forskning

Det er mye forskning rundt personvern, men mye er knyttet til ytringsfrihet eller ivaretakelse av personvernet til sårbare grupper av individer enten det er i skoleverket, eller i fengsel, eller behandlingsapparatet. Når det gjelder tidligere forskning på temaet har jeg ikke funnet noe som reiser spørsmål om årsaken til manglende ivaretakelse av personvernet ligger i styringen og/eller organiseringen. Det jeg har funnet, og som er relevant å bygge videre på, er to arbeider:

I: En studie fra Texas som undersøker i hvilken grad støtte fra ledelsen påvirker forholdet til 6 faktorer som betraktes som sentrale for informasjonssikkehet. (Reddick, 2009) Grunnlaget er funnet ved litteraturstudier, men disse er i hovedsak fra privatsekstor, og fokuset er å undersøke om disse er gyldige og av betydning for offentlig sektor. De 6 fakorene er:

1. **Demografi.** Det fokuseres her på alder, kjønn, utdanningsnivå og hvor mange års arbeidserfaring de ansatte har.

2. **Årsaker til informasjonssikkerhets hendelser.** Det er i litteraturen oppgitt flere alminnelige årsaker til slike hendelser; fra ansattes sluttbrukerfeil til tekniske mangler. Det vises til at det i litteraturen er argumentert for at sluttbrukerfeil er det mest vanlige, og at den sosiale siden av informasjonssikkerhet er blant de største utfordringene.

3. **Miljømessige påvirkninger.** Kulturen i organisasjonen vil påvirke informasjonssikkeheten. Hvis det er en ledelse som fokuserer på avskrekkende reaksjoner i steden for en preventiv tilnærming, vil det kunne påvirke. Informasjonssikkerhet er til syvende og sist et resultat av individuelle handlinger, og en fryktkultur vil kunne resultere i passive medarbeidere.

4. **Informasjonssikkerhets støtte.** Graden av beredskap i organisasjonen vil kunne påvirke graden av suksess.

5. **Type trusler som organisasjonen møter.** Risikovurderinger for å identifisere hvilke type trusler som er mest sannsynlige.

6. **Mekanismer for å møte trussler mot informasjonssikkerheten.** Alt fra virusbeskyttelse og brannmurer til revisjoner og opplæring av ansatte.

Noen av poengene herfra er relevante også for min drøftelse.

II: Kommunal regeletterlevelse. *Illusjoner og realiteter på personvernområdet.* Denne bygger på en undersøkelse rundt det forfatteren kaller "Etterlevelsesillusjonen". (Tranvik, 02/12) Studien har sin bakgrunn i en undersøkelse av hvordan 19 kommuner etterlever reglene i personopplysningsloven med forskrift. Forfatteren hevder at mange kommuner i realiteten ikke oppfyller kravene i den rettslige reguleringen, men at det likevel skapes en illusjon av at de gjør det. Dette kan oppnås fordi reglene gjør det mulig å oppfylle kravene om å dokumentere at man har et system uten at det fungerer, eller er tatt i bruk om man vil. På den måten blir det forskjell på hvilket inntrykk som kan skapes og hva som praktiseres. Atferden harmonerer derfor ikke med verken reglenes intensjon eller det inntrykk man forsøker å skape. Forfatteren angir på side 136 at det er 3 betingelser som må være tilstede for at etterlevelsesillusjonen skal oppstå:

1. Regelverket er kjent for kommunene, og de har en viss vilje til å etterleve det.

2. Kommunenes vilje til å følge reglene er større enn deres evne til faktisk å gjøre det.

3. Regelverket inneholder bestemmelser som gjør det mulig å fremstille forskjellen mellom regelverkets krav til atferd og faktisk regelpraksis som mindre enn hva den i virkeligheten er.

Det foretas ikke noen vurdering av om og eventuelt i hvilken grad de undersøkte kommunene oppfyller kravene knyttet til personvern. Det synes imidlertid som om de alle i større eller mindre grad skaper illusjoner av etterlevelse.

Dette arbeidet er særlig interessant for mitt forskningsspørsmål. Dersom styringssignalene som er gitt i lov og forskrift kan resultere i at det skapes en illusjon om at personvernet er godt, men relaliteten bare er "papir i skuffen", indikerer det behov for endringer i styringssignalene.

Litteratur

Det finnes mye litteratur knyttet til styring og organisering. En del av denne behandler også temaet "institusjonell teori". Koblingen til hvordan dette påvirker medarbeidernes adferd er også behandlet av noen. Denne koblingen er oftest reist av de som har en kritisk tilnærming til hvordan organiseringen og styringen av organisasjoner kan fungere i virkeligheten. Dette gir grunnlag for å drøfte om styringens karakter bør endres fra overordnet til individuelt nivå. Hvordan staten styrer sine organisasjoner, og hvordan organisasjoner styrer sine medarbeidere bør kanskje ikke bygge på samme logikk eller av de samme styringsparametere? Jeg skal i et eget teorikapittel drøfte disse temaene, og knytte de til min hypotese.

2.3 Plan for arbeidet

Jeg skal under denne overskriften redegjøre for hvilke tanker som som har styrt prosessen og modningen av tilnærmingen til forskningsarbeidet. Gjennomgangen vil ende opp med en beskrivelse av hvordan forskningsprosjektet er blitt gjennomført.

Når interessen for problemstillingen oppsto, var tanken å finne organisasjoner som er gode på personvern, og sammenligne dem med organisasjoner som ikke er gode på personvern.

Det er kjent at det er forskjell på hvor gode offentlige organisasjoner er til å ivareta personvernet/konfidensialiteten jf. Datatilsynets undersøkelser. Se f.eks. Kommuneundersøkelsen 2010 – 2011 (Datatilsynet, 2014). Jeg hadde i utgangspunktet tenkt finne noen kommuner som er ulike mht. ivaretakelse av personvernet, men like nok til at oppgaveporteføljen ikke påvirker muligheten for å sammenligne årsaken til ulik måloppnåelse på dette området. I sammendraget i Kommuneundersøkelsen viser Datatilsynet til at:

> *Til tross for det intense arbeidet som har vært lagt ned, svarer kun en knapp majoritet (52 %) av kommunene og fylkeskommunene i redegjørelsen at de har etablert internkontroll for behandling av personopplysninger. Dette er overraskende ti år etter at personopplysningsloven trådde i kraft.*

Videre skriver tilsynet at

> *Når kommunenes besvarelser kontrolleres mot alle kontrollspørsmål, faller andelen som har etablert tilfredsstillende internkontroll til rundt 7 %. Dette er et dramatisk lavt tall.*

Det er ikke funnet dokumentasjon for hvorledes den generelle situasjonen i kommunene er i dag, men på hjemmesiden til Kommunesektorens organisasjon (KS) ligger en rapport (PwC, 2014) som indikerer at situasjonen fremdeles er utfordrende for kommunesektoren. Det uttales bl.a. på side 28:

> «I flertallet av de kommunene vi har intervjuet, ser vi svakheter ved internkontrollen. Med dette mener vi at internkontroll med IOP, herunder arkiv, journalføring og personvern, bør i større grad være en del av kommunens ordinære internkontrollsystem.» (IOP er forkortelse for individuelle opplæringsplaner som oftest er knyttet til elever med utfordringer i skolehverdagen.)

Jeg tenker at når mange kommuner har problemer med å håndtere personsensitivt materiale på en forsvarlig måte, er det neppe grunn for å tro at den generelle tilstanden er bedre.

Det ble gjennomført et intervju med direktøren for Datatilsynet for å få råd om gjennomføringen av forskningsarbeidet, og for å kvalitetsikre at min tilnærming er relevant. Det var også et poeng å reflektere sammen med en som arbeider med problemstillingen til daglig, og som kjenner status på personvernområdet bedre enn de fleste. Min inngang til samtalen var å presentere mitt forskningsprosjekt og formålet med samtalen. Dette ga grunnlag for et opplyst samtykke for å gjøre opptak av samtalen. Jeg redegjorde for forskningsspørsmålet og min hypotese. I den forbindelse var det også naturlig å definere min forståelse og bruk av begrepene "instrumentell" og "institusjonell". Mitt grunnlag for å strukturere samtalen er satt inn nedenfor:

I Datatilsynets årsrapport 2011 (s14) heter det:

"Ledere ser ofte på personvern som et spørsmål om etterlevelse, og ikke som et verdispørsmål for virksomheten."

Dette oppsummerer på en god måte den utfordringen jeg er opptatt av. Men det er ulikheter mellom ulike organisasjoner, og hva er det som er årsaken til det.

Min hypotese er at fokus på institusjonalisering av normer og verdier i tillegg til oppfyllelse av de instrumentelle kravene gir en bedre måloppnåelse.

1. *Hvilke tanker gjør du deg på bakgrunn av det jeg presenterer?*

2. *Kjenner du organisasjoner som kan være egnet å intervjue?*

Jeg fikk bekreftet at temaet i høyeste grad er relevant, og at problemstillingen om etterlevelse av regler og retningslinjer ikke alltid etablerer en verdi knyttet til personvern er sentral. I det videre er innholdet i vår samtale referert.

Han redegjør for at når Datatilsynet er på kontroller/tilsyn, er de ikke bare opptatt av å se på om systempliktene og systemene er på plass, men også om de er implementert i virksomheten. De er opptatt av at informasjonssikkerheten ivaretas som en kulturell verdi. Men det er vanskeligere å måle, slik at hovedfokuset ofte blir å sjekke om dokumentasjonen er på plass. Når de er på stedlig tilsyn blir det likevel alltid gjort intervjuer med sentrale medarbeidere i

virksomheten. Her kommer det lettere til syne om informasjonssikkerheten har en verdi for virksomheten eller om det bare blir en "papirtiger".

Det blir også lagt stadig større vekt på påvirkningsarbeid, - for å skape forståelsen av hvor viktig personvern er. Her har det vært en stor forbedring de siste fire årene. Flere og flere ser verdien av å ivareta sikkerheten til dataene. Omdømme-risikoen ved at data kommer på avveie er stor. Det ser vi ofte i avvisene og media for øvrig. Dette fokuset gjør at det å implementere sikkerhet i alle ledd blir sett på som viktig.

Det økede fokuset henger nok sammen med at stadig mere digitaliseres. Det blir stadig lettere og billigere både å produsere og lagre. Mange systemer er stadig mer komplekse, og det er behov for ganske avanserte datasystemere selv i små virksomheter. De kjøper inn datautstyr, og mange har ikke kompetanse verken til å sette det opp, eller drifte og vedlikeholde systemene. Da blir det et sprik, og ting kan lett komme på avveie.

Det handler om å ha et bevisst forhold til graden av risiko, og etablere flest mulige "fartsdumper" der det er nødvendig. Noe 100 % tett system vil sjeldent være mulig å etablere.

Tilsvarende er det med regelverk; det vil vannskelig kunne ta opp i seg alle eventualiteter. Da er det viktig å ikke tenke slik: *Hvis ikke det er forbudt, er det sikkert lov*. En som har en god personverntenkning inne vil i steden tenke: *Her foreligger det ikke noen tillatelse til dette, og da skal jeg heller ikke gjøre det.*

Vi diskuterte valg av organisasjoner som kan gi et relevant empirisk grunnlag for min problemstilling. Min opprinnelige tanke var å velge noen primærkommuner som er gode, og noen som er mindre gode til å ivareta personvernet. Poenget med det er at de er ellers like nok i forhold til de oppgavene de skal løse, slik at det ikke kan være en årsak for ulikheter i forhold til ivaretakelse av personvernet. Både kommuneundersøkelsen som Datatilynet tidligere har gjennomført (Datatilsynet, 2014), og flere tilsyn i komunesektoren, gir ikke grunn til å tro at det er lett å finne kommuner som er gode på personvern. Det er da neppe lett å finne gode intervjuobjekter som har gode eksempler som kan illustrere spørsmålstillingen jeg reiser. Vi delte en refleksjon om at det trolig bare er de som er gode på temaet personvern som har noe å tilføre mitt forskningsprosjekt. Jeg fikk anbefalt flere offentlige og private organisasjoner som Datatilsynet oppfatter som gode på å ivareta personvernhensyn. Det kunne være interessant å se om det er noen ulikhet mellom offentlige og private organisasjoner når det gjelder tilnærming og arbeidsmetodikk. Mitt overodnede teoretiske grunnlag er likevel

offentlig styring og ledelse, og inneforstått hvordan det offentlige styrer sine organisasjoner. Hvordan det offentlige styrer/kontrollerer ivaretakelsen av personvern i private organisasjoner, og hvordan de private organisasjonene implementerer og forvalter det, blir derved et annet tema.

Jeg valgte å følge de anbefalingene jeg fikk fra Datatilsynet, og har etter det intervjuet to store statlige organisasjoner. Begge forvalter store mengder personopplysninger, og også betydelig med sensitive personopplysninger. Sondringen mellom disse begrepene defineres også nedenfor.

Det var heller ikke hos disse organisasjonene, som Datatilsynet vurderer som blant de beste i klassen, noen bevisst tilnærming til å etablere personvern som en verdi. Begge er imidlertid opptatt av å forvalte eget omdømme, og det er et spørsmål om dette kan sikre personvernet godt nok. Den problemstillingen skal også drøftes. Det var likevel flere interessante funn som kom ut av disse intervjuene. Likevel er ikke dette empiriske grunnlaget tilstrekkelig for å alene belyse det temaet jeg vil undersøke.

På bakgrunn av intervjuene jeg foretok, samtalen med Datatilsynet og funn i andre forskningsarbeider (PwC, 2014), ble planen om en komparativ undersøkelse av noen kommuner forlatt.

I fortsettelsen skal jeg redegjøre for teori, beskrive metoden for forskningen og presentere resultatene fra det empiriske arbeidet. Videre skal det diskuteres hva resultatene fra undersøkelsen betyr, og drøftes opp mot teoriene rundt min hypotese. Endelig skal det vurderes hvilke konklusjoner som kan trekkes, og avslutningsvis se på validiteten ved arbeidet.

3. Teorikapittel

Jeg skal her redegjøre for, og begrunne valg av litteratur. Relevante perspektiver og teorier skal beskrives og forklares. Men aller først skal en del sentrale begreper defineres og avgrenses.

3.1 Begrepsavklaringer

Temaet "personvern" og perspektivet "konfidensialitet" er beskrevet og definert i innledningen (se punkt 2.1.1). Dernest er begrepene "intrumentell" og "institusjonell" sentrale i oppgaven, og trenger en grundig avklaring.

Den **instrumentelle** perspektivet ser på organisasjonen som et objekt, og som et verktøy for å oppnå de mål som er satt. Det etableres formelle strukturer som ikke er personavhengige, og som i seg selv gir føringer for atferd. Videre fastsettes det regler for hvordan beslutninger skal tas der det foreligger flere beslutningsalternativ. Handlingslogikken blir ved det preget av hvilket handlingsrom som gis av de formelle strukturene, og atferden blir preget av en rasjonell kalkulasjon av hvilket alternativ som leder (mest) i retning av målet. (Alvesson & Deetz, 1996)

Styring i det intrumentelle perspektivet betyr å påvirke de forhold som er av betydning for måloppnåelsen. Forholdet mellom de styrende og de styrte blir en type prinsipal – agent relasjon. (Prinsipal-agent-teori dreier seg om hvordan prinsipalen kan fastsette en kontrakt som sørger for at det er i agentens egeninteresse å gjøre som prinsipalen vil. (Idsø)) Dette er en form for mistillitsbasert styring hvor den individuelle handlingen bygger på at konsekvensen fra prinsipalen blir belønning eller straff.

Typiske instrumentelle virkemidler vil være regler, retningslinjer, beskrivelser av prosedyrer og krav til og om systemer.

I det **institusjonelle** perspektivet ses organisasjoner på som subjekter. Organisasjonen består av mennesker som etablerer felles verdier og handlingsregler, og på den måten bygger en kultur. Det søkes oppnådd en legitimitet som sikrer en videreføring av både atferd og av organisasjonen som sådan. (Busch, Vanebo, & Dehlin, 2010)

Styring i dette perpektivet preges av normer og verdier. Handlingsrommet vil være større for den enkelte medarbeider under forutsetning om en forankring i organisasjonens verdier og

normer. Utfordringen kan være at normene kan bli sementerte, og handlingsvalgene kan bli preget av de forventningene som er etablert over tid. Dette kan resultere i en «slik gjør vi det her» holdning, og det er ikke uten videre positivt når endringer er nødvendig. Og i en dynamisk virkelighet vil mangel på tilsvarende utvikling/endring i organisasjonen være uheldig. Man sitter igjen med gårsdagens løsninger på dagens utfordringer. Styringen i et institusjonellt perspektiv vil i større grad være preget av ledelse av mennesker, og ved det endre eller utvikle adferd.

Informasjonssikkerhet er et begrep som allerede er benyttet flere ganger, og som det nå er på høy tid å definere. Informasjonssikkerhet handler om å sikre konfidensialitet, integritet og tilgjengelighet på informasjon. (DIFI, 2014) Det er konfidensialiteten som er fokuset for denne oppgaven. De andre elementene kan likevel være vel så viktige for den enkelte for å oppnå en riktig og etterrettelig behandling hos offentlige myndigheter. «Integritet» handler om å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige. «Tilgjengelighet» handler om at informasjon og informasjonssystemer er tilgjengelige innenfor de krav som er satt til tilgjengelighet. Det er imidlertid ikke «privatlivets fred» som er hensynet bak disse andre to, men hensynet til etterrettelig og rettferdig behandling av/fra offentlige myndigheter. Et særlig spørsmål er om fokus på disse andre perspektivene kan utfordre etterlevelsen av konfidensialiteten, men det vil bare i begrenset grad bli behandlet her. På den annen side kan en spørre om mange skjuler seg bak personvernet for å hindre innsyn i eget arbeid, og på den måten begrenser en optimal samhandling mellom ulike profesjoner. Her er formålet med personvernet forskjøvet fra individet som har krav på hemmelighold, og til profesjonsutøveren som ikke ønsker å bli sett i kortene.

Hvilket innhold personvernet får i møte med offentlige organisasjoner, beror i stor grad på hvorledes offentlige ansatte forvalter personopplysninger. Det er dekning for å si at personvernet er en del av informasjonssikkerheten. «Personvern» handler om den enkeltes rett til et privatliv; det er følgelig individet som er subjektet. Informasjonssikkerhet er noe organisasjoner er pålagt å etablere av hensyn til indivitets rett på personvern. Hvem er det da som er subjektet? Strengt tatt er det fremdeles individet som er subjektet, det er jo bl.a. hensynet til den enkeltes personvern som er hensikten, eller formålet med kravet om å etablere informasjonssikkehet. De som forvalter personopplysinger kan likevel lett tenke at det er virksomheten som er subjekt ved implementeringen av reglene. Det kan medføre at fokuset flyttes fra å verne individets rett til personvern, til organisasjonens eget omdømme.

Skillet mellom personopplysninger og sensitive personopplysninger er av sentral betydning for hvilke krav som stilles til den som skal behandle opplysningene, og hvordan personopplysningene skal behandles. Distingnsjonen mellom disse begrepene er definert direkte i personopplysningsloven § 2.[1] Som man ser av denne legaldefinisjonen er personvern definert ganske generelt som alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Dette f.eks. også omfatte opplysninger knyttet til både bilde og lyd i tillegg til tekst. Begrepet er svært vidt, og vil være omfattende. Dersom en person er identifisert på den ene eller den andre måten, og det gis opplysninger, vurderinger eller omtale, er det en personopplysning.

Ytterligere nødvendige avgrensninger og definisjoner vil gjøres direkte i tilknytning til at begrepene lanseres.

3.2 Litteratur

Det er mye litteratur som omhandler institusjonell teori, og som også reflekterer noe over en intrumentell tilnærming. Jeg har valgt **Organisasjon og organisering** (Busch, Vanebo, & Dehlin, 2010) som bl.a. behandler de ulike aspekter ved institusjonell teori som ett teoretisk fundament. Det legges her vekt på at det ikke er tilstrekkelig for en organisasjon å utføre sine oppgaver på en effektiv måte. For å oppnå legitimitet må organisasjonen også forholde seg til de krav som stilles fra omgivelsene. Det tenkes da på f.eks. de mer eller mindre generelle normene i samfunnet omkring. F.eks. er det uakseptabelt med barnearbeid, bruk av fysisk refselse, skatte- og avgiftsunndragelser m.m. For offentlige organisasjoner vil omgivelsene i

[1] personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson,

sensitive personopplysninger: opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,

b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,

c) helseforhold,

d) seksuelle forhold,

e) medlemskap i fagforeninger.

tillegg særlig kreve en demokratisk forankring, åpenhet og fravær av korrupsjon i større grad enn ellers.

I beskrivelsen av institusjonaliseringsprosessen, det at en organisasjon blir en institusjon, bygger man i stor grad på Philip Selznick (Selznick, 1957). Organisasjonens identitet splittes opp i

- Rasjonelt verktøy og
- Organisk system

Denne sondringen kan minne om det skillet jeg beskriver mellom instrumentell og institusjonell tilnærming. Selznicks teori er imidlertid basert på observasjoner av organisasjoner, i motsetning til teori om organisasjoner. Skillet kan da beskrives slik at den rasjonelle dimensjonen tilfredstiller arbeidsgivers, brukeres eller andre interessenters behov, mens det i den organiske dimensjonen ligger en tilpassning til krav og normer fra omverdenen.

Den organiske dimensjonen vil følgelig ta opp i seg de normer og verdier som er i omgivelsene, og etter noe tid vil organisasjonens verdier ha blitt preget av samfunnet rundt. Denne institusjonaliseringen hevdes å være viktigst for de organisasjoner som har diffuse mål, eller mål som er lite målbare. Poenget er at når målsettingen dreier seg om komplekse og uforutsigbare forhold, vil en tillitsbasert delegering til verdiorienterte medarbeidere fungere bedre enn prosedyrebeskrivelser og rapporteringskrav.

Prosessen vil ofte kunne gå over lang tid, og både ytre og indre press bidrar til denne utviklingen. Det indre presset kan komme ved at medarbeidere blir preget av det samfunnet de lever i, og tar det med seg på arbeid. Det kan også forsterkes eller styres av interne prosesser i organisasjonen (min merknad). Det ytre presset kommer fra eksterne interessenter enten det er kunder/brukere, eller overordnede organisasjoner eller leverandører.

Ingen organisasjon kan fullt ut verne seg mot et slikt press, og disse verdiene kan føre til at det etableres prosedyrer og strukturer, og disse kan få en egenverdi. I forhold til dette er et sentralt poeng at omgivelsene er dynamiske, og interne strukturer må også være det for å opprettholde en legitimitet (min merknad).

Legitimitet er et sentralt begrep i institusjonell teori. Det kan beskrives som summen av at en organisasjon er effektiv og er tilpasset gjeldende normer/verdier både intern og eksternt. På

den måten kan det langt på vei oversettes med omdømme. Dette er min refleksjon av begrepet, og er tilstrekkelig for mitt formål. Legitimiteten eller omdømmet er skapt i en sosial kontekst. Det redegjøres i boken (Busch, Vanebo, & Dehlin, 2010) for at legitimitet kan fremtre på en eller flere av følgende former:

1. Pragmatisk legitimitet. Denne er knyttet til om omgivelsene oppfatter organisasjonen som nyttig i samfunnet.

2. Legal legitimitet er som navnet indikerer knyttet til om organisasjonen overholder de regler og lover som er av betydning for virksomheten.

3. Normativ legitimitet. Denne er knyttet til om omgivelsene anser organisasjonen som ønskelig på bakgrunn av en evaluering av hvordan den driver sin virksomhet på.

4. Kognitiv legitimitet. Det kognitive er knyttet til det erkjente, og til at organisasjonen er som man forventer. Oppfatningen bygger på hva vi tar for gitt. F.eks. at en høyskole har både undervisning og eksamner, mens vi tar for gitt at en brevskole ikke har klasseromsundervisning.

Det å ha et godt omdømme eller en høy legitimitet, er sentralt for de fleste organisasjoner. Det vil også være av betydning å forvalte et godt omdømme slik at det ikke svekkes. Som et ledd i etableringen av et godt omdømme, er det selvsagt nødvendig at det gode arbeidet blir kjent. De som er i organissjonen, eller «bruker» den, vil kunne danne seg en oppfattning. Andre må informeres om organisajonens fortreffelighet. Profilering eller framsnakking av egen organisasjon er vanlig. Det kan være at i iveren om å bygge omdømmet, skryter man litt mer enn det kanskje er dekning for. Det betyr at det kan være større eller mindre sprik mellom det bildet som skapes og de realitetene som finnes.

Organisation och organisering (Eriksson-Zetterquist, Kalling, & Alexander, 2012) som behandler institusjonell teori i forhold til bl.a. både begrepsapparat og filosofisk forankring.

De introduserer temaet ved å angi at det kanskje er slik at det bare er på utsiden at organisasjoner er rasjonelle, og at det i realiten er det institusjonelle som påvirker hvordan og hva som gjøres i organisasjonen. Det gis en presentasjon av utviklingen av institusjonell teori som en del av organisasjonsteorien, og de bringer oss videre hele veien til postmoderne organisasjonsteorier. Det postmoderne drøfter gjerne forholdet til makt og kontroll som et

filosofisk tema. Det er i seg interessante perspektiver, men faller utenfor rammen av denne oppgaven. Jeg nøyer meg med å henvise til f.eks. Foucault som en sentral representant.

Institusjonell teori stiller spørsmål ved forestillingen om den rasjonelle formelle strukturen som et ideal for å oppfylle formelle målsettinger. (Alvesson & Deetz, 1996) Det hevdes at de formelle strukturene i form av organisasjonskart eller prosedyrebeskrivelser ikke nødvendigvis reflekterer hvordan ting faktisk blir gjort. Selv om reglene brytes og det fattes beslutninger som gir andre konsekvenser enn man hadde tenkt seg, lever myten om rasjonalitet nærmest som en norm.

Det presenteres en skandinavisk institusjonell teori. Den tar utgangspunkt i at organisering kan beskrives som en kombinasjon av stablitet og forandring. Normen som beskrives er at selv om stabilitet er en forutsetning for trygghet både hos ansatte og brukere, vil det være at krav om at organisasjonen endrer seg i takt med omgivelsene. Videre reises det spørsmål hvorfor denne dynamiske tilpassingen til omverdnen er så vanskelige å få til dersom forandring er en del av normen. Svaret som gis er at forestillingen om organisasjoner som rasjonelle instrumenter står så sterkt. Forutsetningen for endringer i den logikken er at endringer er et utslag av rasjonelle valg. Derfor blir det ingen endring i henhold til normen før også forutsetningen om at endringen oppfattes som rasjonell, er oppfylt. (min kommentar).

I et pt upublisert kapittel i en bok om styring, tillit og kontroll drøfter forfatteren Hans Christian Høyer bl.a. institusjonalisme i dette perspektivet. (Høyer, upublisert) Kapitellet heter:

Tillit og kontroll – som ild og vann eller som sukker og kanel?

Forholdet mellom tillit og kontroll blir av mange sett på nærmest som motsetninger. Denne oppfatningen bygger trolig på at du ikke kontrollerer en person du har gitt tillit. På den måten blir det å kontrollere en mistillitsbasert sjekk på om den du har gitt tillit viser seg tilliten verdig.

Motsatt ser noen tillit og kontroll som faktorer som kan virke sammen på en god måte. Det beror i stor grad på hvorledes begrepet "kontroll" defineres. Hvis man ser på "kontroll" som det å ha kontroll over hvilke faktorer som påvirker atferd, og eventuelt hvordan disse faktorene kan påvirkes, er det mer positivt enn det å kontrollere at visse aktiviteter blir utført. Når det er sagt er heller ikke begrepet "tillit" entydig.

«Tillit er bra - kontroll er bedre», sa Vladimir Lenin, og i kontekst med dette navnet vil få oppfatte utsagnet som positivt. Og det er gjerne en slik forståelse mange legger i forholdet mellom tillit og kontroll. Når noen kommer på tilsyn for å kontrollere at du har gjort det som kreves, oppfatter de færreste det positivt.

Høyer tar utgangspunkt i at forholdet mellom tillit og kontroll er en kompleks og sammensatt relasjon. (Høyer, upublisert). Begrepene drøfes i en styringskontekst, og diskuterer hvilke utslag det kan få avhengig av om organiseringen er preget av tynn eller tykk institusjonell forståelse. Det legges til grunn at tynn og tykk institusjonalisme er to grunnformer for institusjonsforståelser. Begrepet «institusjonell» brukes her med en litt annen betydning enn den jeg legger til grunn i overskriften på oppgaven der jeg nærmst ser på det som motsetning til «instrumentell». Min bruk av begrepene instumentell eller institusjonell tilnærming vil i Høyers begrepsbruk tilsvare henholdsvis tynn eller tykk institusjonell forståelse. I beskrivelsen av Høyers teori og når det refereres til den, benyttes Høyers begreper. For øvrig i oppgaven begrepene instumentell og institusjonell slik de er definert ovenfor.

Tynn institusjonlisme beskrives som i sin ytterste konsekvens en form for taylorisme. I det ligger en streng og gjennomregulert organisasjon med klare instrukser for aktiviteten, og for alle tenkelige utfallsrom. Ergo en utpreget intrumentell tilnærming (min kommentar). I et slikt regime hevder Høyer at det kan etableres kontrollsystemer for å påse at regler og instrukser blir fulgt, slik at det opprettholdes en velfungerende oganisasjon. Kontrollaktvitetene vil rette seg mot å avdekke feil eller manglende etterlevelse. På den måten er det en etterfølgende kontrollaktivitet som i liten grad kan gripe inn i samtidige prosesser. I et slikt system hevder Høyer at tillit oppnås ved at kontrollen ikke avdekker misligheter. På den måten er det riktig å si at tillit blir en konsekvens av kontrollaktivitet. Dynamikken i tillit – kontroll dimensjonen vil endres avhengig av hva kontrollene avdekker. Ved få avvik i kontrollen, vil tilliten øke, og motsatt. Svakheten med et slikt system er at når uforutsette situasjoner oppstår, er det ingen instruks for hvordan den enkelte skal handle. Dette kan resultere i en handlingslammelse ved at det oppstår en frykt for å bryte med instruksen, eller handle utenfor hva som er regulert. Konsekvensen kan bli at fornuftige handlinger i en ekstrem situasjon ikke blir utført.

På den andre siden beskrives tykk institusjonalisme med at organisasjonen er mer preget av uformelle handlingsnormer internalisert som verdier og normer i de enkelte medarbeiderne enn av instrukser og reglementer. En slik verdiforankring innebærer at den enkelte medarbeider i større grad vet hvilke handlingsalternativ som er «riktig» uten at det er nedfelt

i en instruks. Dette bygger på en tro på menneskets iboende ønske om å handle i overenstemmelse med hva enhver annen fornuftig person ville gjort. (Dette korresponderer med erstatningsretten hvor normen for den forsvalige handling er relatert til hvordan «pater familias» (den gode familiefar) ville handlet. Her ligger årsaken til at man kan bli dømt for sine handlinger selv om man fulgte ordre eller instrukts. Dette kom til uttrykk rettsoppgjøret etter 2. verdens krig både i Norge og i Tyskland. Samme er også grunnen for en del av kritikken som er fremkommet i Gjørvrapporten etter 22. juli (NOU 2012:14, 2014))

Med et tykt institusjonelt syn på organisasjonen vil det med andre ord kunne skapes et rom for spontanitet. Den enkelte medarbeider vil som en følge av verdiforankringen ha en klar oppfatning av hvilket handlingsalternativ som er adekvat i en esktrem situasjon. Det gir også rom for en førtidig refleksjon med sikte på å redusere risiko (min merknad). I en slik logikk vil tillit oppnås ved at det velges ønskelige handlinger. På den måten vil opplevelsen av kontroll komme som en følge av tilliten. Også her vil forholdet mellom tillit og kontroll være dynamisk. Ved at man viser seg tilliten verdig, vil opplevelsen av kontroll øke, men også her vil det motsatte kunne skje.

Høyer diskuterer videre ulike utfall dette kan få for styringsrelasjonen. Der de styrende og de styrte har ulik forståelse av den institusjonelle tilnærmingen i organisasjonen, vil forholdet mellom tillit og kontroll være som ild og vann. Motsatt der de styrende og de styrte har samme forståelse av den institusjonelle tilnærmingen i organisasjonen, vil forholdet mellom tillit og kontroll kunne være som sukker og kanel.

Avslutningsvis konkluderer Høyer med at valget av tynn eller tykk institusjonell tilnærming er avhengig av hvor stor risikoen er for uforutsette hendelser i den enkelte organisasjon eller tjeneste område. Det synes som han konkluderer med at den optimale situasjonen alltid er der både den styrende og den styrte har en tykk institusjonell oppfatning av tillit og kontroll.

Min merknad: Jeg tenker at det neppe er noen fasit på at den ene eller det andre tilnærmingen alltid er best. Slik jeg ser det vil oppgaveporteføljen, og risikoen for uforutsette situasjoner, være bestemmende for valget. Tilnærmingen og vurderingene kunne variere avhengig av hva som skal styres, og hvilken tjeneste som skal leveres, eller hvilken verdi som skal oppnås. Det er forskjell på utfordringene der staten styrer sine underordnede etater og virksomheter, og styringen intern i den enkelte organisasjon. Og om tilsvarende styringslogikk uten videre kan videreføres overfor den enkelte medarbeider. Tilsvarende vil utfordringene være ulike om det

er en type «samlebåndsproduksjon» eller om det er verdien «personvern» som skal skapes. Dette er perspektiver som gir grunn for ytterligere diskusjoner om forholdet mellom tillit og kontroll.

Videre er grunnlaget for beslutninger, hvordan de fattes, og begrunnelsen for veivalg interessant. Både i forhold til valg av organisering, men også hvordan beslutninger og vurderinger gjennomføres inn i organiseringen og inne i organiasjonen.

Det er i hovedsak elementer fra tre bøker hvor disse perspektivene er behandlet jeg vil bygge min drøftelse av denne dimesjonen på:

James G. Mach: Fornuft og forandring – *ledelse i en verden beriget med uklarhet.* (Mach, Fornuft og forandring, 1995, 2. utgave 2008). Det er tre bjelker i Mach' tenkning:

1. Verden er tvetydig og komplekst sammensatt
2. Prosesser som sudieobjekt framfor resultater
3. Rasjonalitetsmyten

Mach spør om hvorfor myten om rasjonelle valg står så sterkt. Han gir noen mulige årsaksforklaringer:

1. Underbygger politiske og økonomiske filosofier og
2. Dermed våre politiske og økonomiske institusjoner
3. Underbygger indiviualisme
4. Begrunner raske endringer
5. At tradisjon må vike for viljekraft

Daniel Kahneman: Tenke, fort og langsomt. (Kahneman, 2012) Boken redegjør for at vår måte å tenke på bygger på to systemer:

1. Raskt, intuitivt og følelsesdrevet eller

2. Langsomt, rasjonelt og logisk

Begge systemene er nødvendige, og begge har sine svakheter. Ved å være seg bevisst de to systemene, og hvordan de virker sammen, kan en oppnå en bevissthet som leder til bedre avgjørelser.

På den måten tar denne boken også i noen grad tak i forestillingen om det rasjonelle menneske, men viser at det ikke er mulig på grunn av kapasiteten å alltid være rasjonell. Intuitiv tenkning er effektiv og ofte riktig. Dersom vi er bevisst på når vi bør velge å benytte det rasjonelle tenkesettet, vil vi kunne øke andelen med "riktige" avgjørelser.

Nils Brunsson: Mechanisms of Hope (Brunson, 2006) *Maintaining the Dream of the Rational Organization.* Forfatteren er blant annet opptatt av den intensjonale dimensjonen i rasjonaliteten. Han hevder at rasjonalitet er en intensjonal form for intelligens. Rasjonell kan forklares med fornuftsmessig og gjerne relatert til handlinger. Mens det intensjonale aspektet retter seg mot et objekt. Med en slik forståelse skilles det mellom det fysiske og det psykiske virkelighetsbildet. (Svendsen)

Hykleri og reformer/endringer er to måter å håndtere en systematisk uoverensstemmelse mellom hvordan ting burde være og hvordan de er, hevder Brunson. Når slike endringer gjenomføres er ideen at det blir bedre harmoni mellom hva vi vil, sier og gjør. Erfaring viser at dette ikke er det mest vanlige resultatet. Likevel blir håpet om en bedre virkelighet, eller organisasjon, sittende igjen til tross for at det ikke ble realiteten, eller er oppnåelig. Så selv om ideen om en rasjonell tilnærming til endring ikke lykkes, har vi likevel håpet i behold. Det i seg selv sørger for en stabilitet som har en verdi. Litt av Brunsons poeng er at håpet kan bidra til å opprettholde idealet om en rasjonell organisasjon, selv om rasjonaliteten i seg selv feiler.

Både James March og Daniel Kahnemann er opptatt av hvordan vi mennesker gjør valg. Med ulik innfallsvinkel drøfter de at idealet om det rasjonelt tenkende og besluttende menneske tidvis er en illusjon. Kahnemann er mest opptatt av individet og forholdet mellom intuisjon og rasjonalitet. March er også opptatt av om beslutninger i organisasjoner er rasjonelle, og gir noen forklaringer og noen hypoteser for hvorfor de ikke alltid er det.

Det er selvsagt litt nedslående om vårt selvbilde om å være rasjonelt agerende mennesker ikke holder stikk. Nils Brunson synes i sin bok å erkjenne at fullstendig rasjonalitet sjeldent er mulig. Dette beror på både begrenset kapasitet for å foreta alle nødvenige vurderinger til en

hver tid, men også på at vår evne til å spå om framtiden er begrenset selv om alle opplysninger som er nødvenig for en rasjonell tilnærming er til stede. Han mener likevel at det er av betydning å beholde håpet og drømmen om en rasjonell organisasjon. Det kan være at bedre alternativ for organisering og styring ikke er tilgjengelig. En kan også spørre om selve bevisstheten om organisasjonens utilstrekelighet i seg selv gjør den bedre.

Samlet sett vurderer jeg at mitt utvalg av materiale gir grunnlag for å se på mulige årsaker til manglende etterlevelse av personvern, og drøfte mulige tilnærminger som kan bedre ivaretakelsen av personvernet.

3.3 Metode

Forskningsmetode

Utgangspunktet for forskningsprosjektet er min undring over hva som er årsaken til at personvernet blir ivaretatt med ulik grad av sukess i offentlige virksomheter. Suksess i denne sammenhengen vil være at organisasjonen evner å gi borgerne personvern, og har få eller ingen avvik. Svaret på hvorfor det er forskjeller, må det være mulig å finne ved å undersøke hvordan det arbeides med personvernspørsmål i de ulike virksomhetene.

Den empiriske undersøkelsen er baseret på dybdeintervjuer hos to organisasjoner i tillegg til Datatilsynet. Dette ville jeg gjøre opptak av, og det var derfor nødvendig med en melding til Norsk samfunnsvitenskapelig datatjeneste (NSD). Årsaken er at jeg skulle gjøre opptak på et elektronisk medium. Jeg så ikke for meg at undersøkelsen i seg selv ville omfatte personopplysninger eller annet sensitivt materiale. Slik melding til NSD ble sendt. Tilbakemeldingnen konkluderte med at prosjektet ble ansett som meldepliktig, og at meldingen nå var tilfredsstillende utført.

Det å gjøre opptak og senere transkribere teksten, er en tidkrevende prosess. Enkelte forskere leier hjelp til slik transkribering. Jeg valgte å gjøre dette selv, fordi jeg ønsket å kjenne hele prosessen på kroppen. I etterkant ser jeg at dette var et riktig valg. Min erfaring er at analysen ikke er noe man starter med etter at man har transkribert intervjuene. Tolkninger og refleksjoner rundt det innsamlede materialet har fulgt meg i hele forskningsprosessen. Først under selve internvjuet, senere mens jeg transkriberte og ved lesing av det ferdig transkriberte

materialet. Refleksjonene modnet underveis og ble foredlet ved lesning av det ferdig transkriberte.

Forskningsprosess

Temaet som er valgt er personvern. Det er konfidensialiteten som jeg vil avgrense studieobjektet til. Det er neppe tvil om at personopplysninger fra tid til annen kommer på avveie, eller at «noen» snoker i journaler eller registre uten at de har anledning til det. Tilgang til personopplysninger krever samtykke, lovhjemmel eller det som gjerne kalles «tjenstlig behov».

Problemstillingen er: Hvorfor er personvernet så dårlig ivaretatt i offentlige organisasjoner i Norge? Spørsmålet er videre om det er ulikheter mellom organisasjoner, og om årsaken kan ligge i ulik tilnærming til styring og organisering. På bakgrunn av anbefaling fra Datatilsynets direktør valgte jeg to statlige organisasjoner som ble oppgitt å være gode på personvern. Spørsmålet er om disse intervjuene gir et tilstrekkelig bilde som kan gi grunnlag for analysen.

Etter samtaler med Datatilsynet og de to virksomhetene viste det seg at noen bevissthet eller noe planmessig arbeide i forhold til å etablere personvern som en egen verdi i organisasjonene, ikke er fremtredende. Det kan likevel være at fokuset på risikoen for omdømmetap, etablerer en verdiforankring utover den instrumentelle etterlevelsen. Begge organisasjonene oppga godt omdømme som essensielt for legitimitet og eksistensberettigelse. Spørsmålet videre blir da om fokuset på vern av omdømme kan kalles en institusjonell tilnærming?

Når intervjuene i to organisasjoner som er oppgitt å være gode på personvern, ikke avdekket noen bevisst holdning til forholdet mellom intrumentell og institusjonell tilnærming, finnes det neppe mange andre som har det heller. Det var kanskje heller ikke å forvente en direkte refleksjon i forhold til disse begrepene, men en verdiforankring kunne man forvente. At det var en refleksjon rundt hvem som skal vernes. Er det individets rett på personvern, eller er det organisasjonens omdømme som står i sentrum?

Dette endrer forskningsprosessen ved at analysen i større grad må basere seg på teori i forhold til temaet. Det må ses på de utfordringene som er avdekket i annen forskning og undersøkelser rundt ivaretakelsen av personvern, og drøfte om institusjonell teori kan bidra til å peke på mulige løsninger på utfordringene. Det er også i den sammenhengen interessant å se på om enkelt individers praksis rundt de instrumentelle statlige føringene kan ha betydning.

Forskningsdesign

I og med at intervju undersøkelsen i begrenset utstrekning belyste min hypotese, er det behov for å forankre større del av drøftelsen i teori. Her er det særlig tre spørsmål som det er sentralt å ta utgangspunkt i:

1. Hva er problemet?
2. Hva er årsaken til problemet?
3. Hva er løsningen på problemet?

Mitt utgangspunkt var en komparativ tilnærming, men det gir liten mening når det ikke er identifisert noen virksomheter med en tung institusjonell tilnærming på personvernområdet. Siden komparasjon ikke er mulig, vil dette prosjektet ha mer preg av en diskusjon mellom teori og praksis. Det vil si forholdet mellom mine teoretiske antakelser om det gode ved institusjonelle tilnærminger, og hva som hevdes i litteraturen, og refleksjonsnivået rundt dette i organisasjonene jeg studerer.

Problemformulering

Forskningsspørsmålet må i noen grad omformuleres. Problemet er at det er begrenset hvor mange som har etablert verdien «personvern» i organisasjonen, og hos den enkelte medarbeider. Er årsaken til det, eller en del av forklaringen, den instrumentelle styringen fra overordnet nivå, den lokale styringen innad i organisasjonen, eller er det andre mulige forklaringer. Svaret på dette siste spørsmålet vil kunne gi grunnlag for å peke på en eller flere mulige løsninger på problemet.

4. Resultater

Her skal resultatene fra undersøkelsene presenteres og diskuteres.

Det er gjennomført to semistrukturete intervjuer med statlige organisasjoner, i tillegg til samtalen med Datatilsynet.

Begge organisasjonene har bedt om at deres identitet forblir hemmelig. Årsaken er at de opplever det ubekvemt å erkjenne at de har forbedringspunkter i deres informasjonssikkerhetsarbeid. Jeg har ingen betenkeligheter med å unnlate å identifisere hvem disse informantene er. Organisasjonene kan beskrives tilstrekkelig for mitt formål uten at identiteten avsløres. Jeg benevner disse organisasjonene i det videre som A og B.

Jeg hadde den samme tilnærmingen i møte med begge organisasjonene. Først informasjon om mitt prosjekt, og innhenting av samtykke til deltakelse, og for å gjøre opptak av samtalen. Begge organisasjonene ble først kontaktet per e-post som ledet fram til en avtale om et personlig møte. I begge tilfellene hendvendte jeg meg til personvernombudet i organisasjonen, og ytret også ønske om å møte noen med et lederansvar for informasjonssikkerhet. I ingen av tilfellene fikk jeg noen samtale med andre enn personvernombudet. Det er ikke grunnlag for å spekulere i årsaken til det, og det gir ingen grunn for å anta at det er uvilje mot å delta i min undersøkelse. En like sannsynlig årsaken er ferietid, andre mer presserende oppgaver, eller en generell prioritering i forhold til all verdens forespørsler om undersøkelser som som ramler inn. Men en mulig årsak kan også være at temaet ikke er prioritert.

Det ble som nevnt lagt opp til et semistrukturert intervju og intervjuguiden er limt inn nedenfor:

> *Presentasjon av forskningsprosjektet, avklaring av begrep og hvilken betydning som legges til grunn. Informasjon som er nødvendig grunnlag for at et informert samtykke kan gis til deltakelse i undersøkelsen.*
>
> 1. *Hva er din posisjon i organisasjonen, og hva er din rolle i informasjonssikkerhetsarbeidet*
> 2. *Konfidensialitet og lederforankring*
> 3. *Konfidensialitet og teknisk skjerming*
> 4. *Konfidensialitet og rutinebeskrivelser/reglementer mm*

5. *Konfidensialitet og forholdet til tjenstlig behov*
6. *Hva når tjenstlig behov og taushetsplikt står mot hverandre*

a. Særlig i forhold til eksterne

7. *Avvikshåndtering*
8. *Hva gjøres for å etablere verdien «personvern» i organisasjonen*

Kan jeg ta kontakt med deg om jeg har oppfølgingsspørsmål?

Organisasjon A

Dette er en landsdekkende virksomhet med desentraliserte og delvis underordende kontorer. Virksomheten er en sentral samfunnsaktør, og har stor betydning for samfunnsutviklingen på sitt område. Personvernombudet er en sentral fellesfunksjon for hele organisasjonen. Ombudet deltar i overordnet ledergruppe, og rapporterer direkte til øverste leder selv om personalansvaret for vedkommende er plassert på et nivå under.

Denne virksomheten har en historie som går flere ti-år tilbake, og har alltid forvaltet personopplysninger. Særlig gjelder dette myndighetsdelen av oppgaveporteføljen. Likevel er et systematisk abeid relatert til informasjonssikerhet og personvern av nyere dato. Det gjenstår også en del arbeid før kravene i personopplysningsloven med forskrift er oppfylt.

Styringen av den desentraliserte delen av virksomheten går via toppledelsen. Verken personvernombudet eller andre fagledere har noe formelt grunnlag for å kreve eller pålegge noe lokalt uten via toppledelse og/eller lokal leder. Denne formen for "nessekonge"-organisering er trolig krevende i forhold til endrings- og implementeringsarbeid. Personvernombudet bekrefter at det er en ganske komplisert organisasjon å nå frem til eller ut til.

Informasjonssikkerhetsarbeidet er forankret hos toppledergruppa. Det er en åpen vei inn for å informere om arbeidets status. Noe mer uklart i hvilken grad det er vilje til på ta grep for å påskynde arbeidet ved pålegg eller andre føringer fra topplеder. Informasjonssikkerhet ses på som en del av styringssystemet, og så ligger internkontrollen på siden eller over for å påse at det gjøres det som de sier de skal gjøre. Man er i startfasen med å etablere styringssystemene for informasjonssikkerhet.

Det er en del teknisk skjerming for tilgangskontroll basert på rolle i organisasjonen. Dette er et teknisk spørsmål som informanten ikke kan være presis på. Mye ligger åpent for alle ansatte, og det er lite begrensninger på tilgjengelighet innad.

Det finnes en del rutinebeskrivelser, men ingen overordnet håndbok eller lignende for informasjonssikerhet. Personvernombudet har imidlertid laget en sjekkliste, eller huskeliste for hva man må tenke på når man jobber med personopplysninger. Korte forklaringer på hva som er hva, f.eks. hva som er personopplysninger og hva som er sensitive personopplysninger.

Organisasjonen har en taushetserklæring, og alle nytilsatte gjennomgår en opplæring hvor en bolk er informasjonssikkerhet.

Avvikshåndtering er det personvernombudet snakker mest om internt i virksomheten. Likevel er de ikke gode på å rapportere avvik. Det dukker opp spørsmål om det må være avvik fra en rutine e.l., eller kan det være avvik også ellers? Hva er et avvik som skal meldes inn, og hva er tysting? Kan jeg gå utenom min leder? Når en så skal ta skrittet å melde et avvik, hvor og hvordan gjøres det. Virksomheten har en rullgardin på intranettet som det står "meld avvik" på. Tydeligere kan det ikke gjøres, likevel er det mange som ikke finner denne. Her er det 6 ulike alternativ som omfatter bl.a. HMS, kvalitetssystemet, sikkerhet og personvern. Dette er et fellesområde for hele organisasjonen. Det synes likevel som det i noen grad er etablert ulike måter å melde avvik på i de ulike fagmiljøene parallelt eller alternativt til denne ordningen. Samordning er en utfordring i en stor organisasjon.

På den annen side får personvernombudet også en del henvendelser direkte til seg av typen "bekymringsmeldinger". Det kan være de som undrer seg over at de har tilgang til materiale de tenker de ikke burde ha, men som ikke melder dette som avvik. Dette vitner om en bevissthet, men synliggjør også et sprik i organisasjonen.

En møter ofte problemstillingen med kryssende interesser. Særlig gjelder dette i forhold til eksterne. Internt er det vanskelig å forklare begrenset tilgang ut fra tjenslig behov, mens enhver ekstern kan be om innsyn i det samme. Både overfor andre offentlige instanser, og i forhold til almenheten generelt, er virksomheten særdeles serviceminded. Det har vært en nokså utstrakt praksis med deling av opplysninger, men det er strammet inn nå. Når slike ønsker eller behov fra andre om å få tilgang til taushetsbelagte opplysninger mottas nå, er holdningen betydelig mer restriktiv. Poenget med en del innsamlet sensitivt materiale er for at

orgnisasjonen skal kunne ivareta sitt samfunnsoppdrag. Noen refleksjon over at dette materialet også kan være av avgjørende betydning i andre sammenhenger, synes begrenset.

Det mest interessante for meg er selvsagt spørsmålet om hva som gjøres for å etablere personvern som en verdi i virksomheten. Som Datatilsynet viser til er personvern ofte bare et spørsmål om etterlevelse. Det ligger implisitt i denne utalelsen det er ønskelig at personvernarbeidet hos den enkelte organisasjon resulterer i noe mer. Jeg slutter meg til en slik vurdering. Etterlevelse alene vil ikke være tilsrekkelig i de tilfellene regelene ikke fullt ut tar opp i seg alle mulige utfallsrom. Da er det avgjørende at hensynet til privatlivets fred ivaretas på den måten som er nødvendig.

Informanten i organisasjon A opplyser at noen slik tilnærming ikke er en del av strategien. Det vises til at å bevare omdømmet er et viktig mål, og en rettesnor for å passe på taushetsplikten. Det virkemiddlet som brukes er misjonering av temaet der det gis mulighet. Ellers er ambisjonen å få med både HR og kommunikasjonsavdelingen på det videre arbeidet. Det er en sentral refleksjon at IT også er sentrale i arbeidet, men at de ikke kan ha noe selvstendig helhetlig ansvar.

Organisasjon B

Dette er også en stor statlig organisasjon med en lang historie bak seg. Den er underlagt statlig styring, men er faglig uavhengig. Geografisk er den plassert på mer enn ett sted, men det synes ikke å ha noe med oppgaveutførelsen å gjøre. Organisasjonen er en viktig premissleverandør for andre samfunsaktører med betydning for samfunnsutviklingen. Den har både sikkerhetshåndbok og en IT-sikkerhetshåndbok.

Personvernombudet er organisert som en selvstendig funksjon, men med tette bånd til toppledelsen. Det er organisert som en integrert del av internkontrollen, men med selvstendig rapportering til toppledelsen. Ombudet er plassert i juridisk seksjon, og har også andre oppgaver der. Det er således ikke en 100% stilling, men det er flere som har arbeidoppgaver knyttet til informasjonssikkerhet. Virksomheten fikk totalt 4 jurister uken etter mitt besøk. Denne organisasjonen har hatt personvernombud i flere år, og har også før det hatt et stort fokus på slike spørsmål. De ser noe bredere på sikkerhet enn bare informasjonssikkerhet, og har etablert et sikkerhetsteam hvor personvernombudet er med. I tillegg består sikkerhetsteamet av en bygningstekniker for å vurdere skallsikringen, og en sikkerhetsrådgiver fra IT-seksjonen som ser på den tekniske IT sikkerheten.

Både sikkerhetsrådgiveren og pesonvernombudet sitter i administrasjonsdirektørens stab. I forhold til løpende ting rapporteres det her, men det er en rett linje til toppleder i informasjonsikkerhetsspørsmål når det er påkrevd.

Virksomheten ser på sikkerheten som en trefotet krakk: personell-sikkerhet, informasjonssikkerhet og fysisk sikkerhet. Det er etablert god teknisk sikkerhet, men kommer man inn i bygget og kan koble seg på der, så har man passert en del av barierene som man vil møte dersom man prøver å koble seg på utenfra. Det er derfor viktig at ikke hvem som helst kan komme seg inn i bygget. Også av hensyn til dataskjermer som kan vise opplysninger, og utskrifter som kan ligge tilgjengelige, er denne kontrollen viktig.

Tilsvarende har også egne ansatte på oppdrag eller arbeid utenfor huset en begrenset tilgang. Dette gjelder også for hjemmekontor hvor løsningen forutsetter dobbelt autentsisering, og hvor den enkeltes PC blir redusert til en terminal. Det betyr at det ikke kan hentes ut informasjon for lokal lagring eller utskrift. Det er altså bare en lese og registrerings tilgang.

Det er en bevisst holdning til forholdet mellom tjenstlig behov og taushetsplikt. Alle i virksomheten har signert en taushetspliktsavtale, og har på den måten en lovlig tilgang til alt materiale, men denne begrenses av en vurdering rundt tjenstlig behov. Informanten forteller at den tekniske tilgangsstyringen mange stederer er på individnivå, og at det gis tilgang etter behov. Det er den enkelte seksjonssjef som "eier" dataene, og ingen andre i huset har lovlig tilgang uten at det er godkjent av den som er fagansvarlig. På den måten er organiseringen svært sektorisert.

Databaseadministratorer må ha tilgang til det meste for å kunne utføre sine arbeidsoppgaver. De er imidlertid registrert som personlige brukere og har ikke en rollebasert tilgang. På den måten blir alt en person foretar seg logget, og det har trolig en oppdragende effekt.

Rutinen for å fjerne tilgangen når en arbeidstaker slutter, eller roterer internt kan glippe, og det arbeides med en bedre oppfølging av dette.

Riskovurderinger er en del av tilnærmingen, og er bakgrunn for den strenge tilganskontrollen både fysisk og teknisk. De har fokus på avvikshåndtering, og det ligger et verktøy for det direkte på intranettet i form av et word skjema. Det meldes relativt få avvik, og det antas at det er flere avvik enn de som blir meldt. Avvik behandles av sikkerhetsteamet som vurderer hva som er gjort for å begrense skaden, og for å gjenopprette normaltilstand. Ytterligere tiltak

blir eventuelt iverksatt, og det vurderes om dette er et engangstilfelle eller om det er en systemfeil. Avvik kan meldes anonymt; det viktigste er at sikkerhetsteamet blir kjent med avviket.

Når det gjelder spørsmålet om personvern som verdi i organisasjonen, vises det til at avvik som blir kjent ville være helt ødeleggende for omdømmet og organisasjonens tillit. Dette vil lett kunne begrense innsamling av opplysninger, og på den måten ødelegge organisasjonens leveranser. Virksomheten selger ikke sine produkter, men tilliten til produktenes etterrettelighet er sentral i forhold til tilliten og i siste instans virksomhetens eksistensberettigelse.

Alle ansatte blir kurset når de starter, og alle blir ved det gjort oppmerksomme på at virksomheten er avhengig av tillit for at de skal ha en jobb.

Personvernombudet gir uttrykk for at de gjerne skulle hatt med ressurser og mer tid for å gjøre jobben enda bedre.

Hva er så de **konkrete resultatene**, eller funnene, fra undersøkelsen?

Organisasjon A har relativt nylig etablert ordningen med personvernombud og har startet på en mer overordnet systematisk tilnærming til informasjonssikkerhetsarbeidet. Personvernombudet er en del av toppleders stab, og lederforankringen er således ivatetatt. De har i årtider forvaltet store mengder personvernmateriale, men med en noe fragmentarisk tilnærming til temaet. Det er ikke kjent at organisasjonen har hatt store utfordringer i forhold til brudd på konfidensialitet verken intern eller eksternt.

Organisasjonen erkjenner at de mangler en del systemer og struktur for at informasjonssikkeheten skal være ivaretatt i henhold til bestemmelser i lov og forskrift. Avviksmeldinger fungerer ikke etter intensjonene, men noen bekymringsmeldinger vitner om om en bevissthet hos enkelte medarbeidere. Organisasjonens hierakiske oppbygning med sentral enhet og desentraliserte enheter gir en utfordring med kommunikasjonen. Den bærende verdien i forhold til personvernet er risikoen for omdømme tap for organisasjonen selv.

Jeg tolker opplysninger i intervjuet slik at det er få kjente brudd på konfidensialiteten til tross for at det mangler en del før den overornede systematiske tilnærmingen til

informasjonssikkehet er på plass. Organisasjonens medarbeidere har en stor faglig integritet og personopplysninger er bare av interesse dersom de er av betydning for den faglige tilnærmingen. Det innebærer at det er gjennomføringen av det faglige oppdraget som står i sentrum. Jeg tolker det slik at det er et stort fokus på konfidensialitet, men at personopplysninger bare er er en del av helheten.

Den desentraliserte strukturen hvor styringen for en stor del går via toppledelse, hemmer endringer av det faglige fokuset. Dette vil også slik jeg ser det, kunne vannskeliggjøre en systematisk implementering av personvern, informasjonssikkehet eller andre nye krav til organisasjonen som sådan.

Jeg oppfatter ikke at organisasjonen har noe bevisst forhold til personvern som en verdi for enkeltindivider. Den verdien som gjør at konfidensialiteten opprettholdes, er risikoen for omdømmetap for organisasjonen selv. Det er i seg selv en verdi, og representerer således en institusjonell tilnærming. Om dette er fullgod erstatning, behandles nedenfor.

Organisasjonen besitter en del personopplysninger som andre offentlige etater etterspør. Det kan være både skattemyndigheter, politiet og andre. Her oppfatter jeg at det er blitt en øket bevissthet på at personopplysninger bare skal fylle det formålet de opprinnelig er innsamlet for, og senere slettes. Den informasjonen som tidligere i noen grad fløt fritt, er sterkt begrenset. Det finnes eksempler på at det å formidle personsensitivt materiale ville være en fordel for den som har krav på hemmelighold. Refleksjoner om denne type utfordringer synes å være begrenset, og opplysningene vil i noen grad forbli i organisasjonens fagmiljøer som bare ser det som er faglig relevant.

Det framstår som konfidensialiteten er rimelig godt ivaretatt til tross for mangler ved den systematiske tilnærmingen. Bevisstheten om å ta vare på omdømmet som den herskende verdien i organisasjonen, synes langt på vei å være tilstrekkelig. Det som er benevnt som en "aktiv legitimitetsforvalning" (Busch, Vanebo, & Dehlin, 2010), ser ut til å være institusjonalisert i organisasjonen. Det er ikke alltid at en slik bevissthet om å profilere egen legtimitet resulterer i full harmoni mellom bildet som skapes og realitetene i organsiasjonen. I dette tilfellet har fokuset på omdømmet, og bevisstheten om behovet for å ta vare på organisajonens legitimitet, også hatt betydelig intern effekt.

Organisasjon B har i mange år hatt et personvernombud. De har en bredere tilnærming til sikkehet og informasjonssikkehet enn de fleste. De har etablert ett sikkerhetsteam som

ordinært rapporterer til nærmeste leder, men som har en direkte linje til toppleder når det anses formålstjenlig. De ser på sikkerheten som en trefotet krakk: de fokuserer på både personell sikkehet, informasjonssikkehet og fysisk sikkerhet. "Det holder ikke med fysisk og teknisk sikkerhet hvis du bare ansetter kjeltringer" (sitat fra informanten). Det vitner om en refleksjon over betydningen til den enkelte medarbeider, og hans eller hennes kunnskaper og holdninger. Dette vitner om en viss istitusjonell forståelse av organsasjonen. De har et oppegående system for avvikshåndtering, men antar at det likevel ikke er alle avvik som blir rapportert.

Denne organisasjonen har stor bevissthet på sikring av bygget, og en streng adgansgkontroll. Ingen eksterne slipper inn uten at de blir hentet av en ansatt, og fulgt tilbake til utgangen. De har en sikkerhetshåndbok som er under revidering for å bedre strukturen. I tillegg har de en egen IT-sikkehetshåndbok for det IT steller med. De har en tilgangsstyring på individnivå, og mye logging av hva mange medarbeidere foretar seg digitalt. Tilgangsstyringen ved ekstern oppkobling er stramt teknisk styrt. Her er det intrumentelle i fokus ved etablering av strenge systemer.

Jeg oppfatter at denne organisasjonen har et stort og bevisst fokus på personvern og konfidensialitet. Det skilles ikke på personopplysninger og annet konfidensielt materiale. Alt behandles etter samme strenge regime. I forhold til personvernet for egne ansatte synes ikke det å være underlagt samme fokus. I hvert fall er ikke det noe som personvernombudet fokuserer på.

Verdiforankringen i denne organisasjonen er tilsvarende som for organisasjon A. Det er bevistheten om å bevare eget omdømme, og et fokus på å forvalte egen legitimitet, som står i sentrum. Samme refleksjon og referanse som for organisasjon A gjør seg derfor gjeldende også her.

Organisasjon B har et kursopplegg for nyansatte som bl.a. poengterer betydningen av konfidensialitet som en forutsetning for å opprettholde organisasjonens legitimitet. Det framstår som om det settes av mer ressurser for å ivareta sikkeheten i organisasjon B enn i A, men personvernombudet gir likevel uttrykk for at ytterligere ressurser hadde vært ønskelig for å utføre oppgaven enda bedre.

Felles vil jeg peke på organisasjonenes utfordringer slik jeg ser det. Begge ivaratar konfidensialiteten godt. At de begge har mangler, om enn i ulikt omfang, i forhold de lovbestemte aktivitetspliktene, synes ikke å utfordre konfidensialiteten. Manglende

dokumenasjon av systemer, risikoanalyser, avvikshåndtering m.m. vil kunne resultere i avvik ved et tilsyn. Det kan være grunn for å spørre om statens styring av aktiviteter, og krav om etablering av rutiner er en optimal organisering i ett hvert tilfelle er formålstjenlig. Personvernet synes i disse to organisasjonene uansett rimelig godt ivatetatt.

At de har fokus på sitt eget omdømme i steden for individets krav på vern, - representerer det noe problem? Ja jeg tenker at det gjør det, selv om hensikten eller målet langt på vei oppnås. Når fokus er rettet mot å opprettholde et bilde på egen fortreffelighet kan en lett glemme at personvern er en rett for enkeltindvidet. Det kan tenkes situasjoner der omdømmet blir utfordret, og hvor den enkeltes personvern ofres hvis man tror det kan bidra til å opprettholde omdømmet. Dersom det skjer, kan det ses på som en konsekvens av fokus på eget omdømme fremfor individets rett på personvern.

5. Diskusjon

Jeg starter dette kapittelet med noen innledene refleksjoner om personvern og en redegjørelse for styringssystemet på statlig nivå generelt. Hvordan disse styringssysignalene operasjonaliseres hos mine informanter drøftes konkret i forhold til disse. Dernest skal jeg drøfte funnene fra samtalen med Datatilsynet og fra intervjuene opp mot problemstilling og hypotese.

Hvordan styringen slår ut og kan fungere skal jeg drøfte på tre nivåer:

1. Det overordnede statlige nivået
2. Organisasjonsnivået og
3. Det individuelle nivået

Fortløpende skal jeg diskutere hvordan dette korresponderer med teorien fra den litteraturen jeg har redegjort for, og de funnene som er gjort i de andre forskningsarbeidene jeg har bragt inn i oppgaven.

Innledning

Jeg tenker at de fleste mennesker har en oppfattning av hva som ligger i begrepet "personvern". Hvor presis oppfatningen er, og hva de tenker er personlige opplysninger, vil nok variere mye. Når en ser hva mange deler på sosiale medier kan en lett få en forestilling om at mange er bevisstløse i forhold til dette, men det kan like gjerne bero på uvitenhet om rekkevidden av delingen. Refleksjonen om hva som kan/bør deles om andre, kan nok med fordel bli bedre.

Når det gjelder det offentliges ivaretakelse av den enkeltes personvern er nok bevisstheten hos den enkelte borger er større. Det kan være at deler av personsensitivt materiale hos offentlige instanser er mer infamerende, men jeg tror ikke det er hele forklaringen. Uansett er det en viktig erkjennelse at forventningene til det offentliges ivaretakelse av den enkeltes personvern er høyere enn de refleksjonen den enklete gjør seg ved håndtering av eget personvern. Og slik skal det også være, tenker jeg. Det offentlige må ivateta både hensynet til den enkelte og til fellesskapet som sådan. Det betyr f.eks. at offentlige virksomheter ikke kan hindre at privat personer sender sensitive personopplysninger i en e-post, men må likevel behandle det på foreskrevet måte når de får det i hus.

Et perspektiv det kan være verd å ta med seg her er det faktum at alle offentlige tjenestemenn også er privatpersoner. Kan den avslappede holdningen som mange generelt har til personvern på den private arenaen, også kunne påvirke den profesjonelle håndteringen av personvernspørsmål? Det kan være at noen tar med seg jobben hjem og noen tar med seg privatlivet på jobben? Imidlertid er det ingen indikasjoner på at dette er en utbredt utfordring. Det er likevel grunn for å være besvisst også denne mulige utfordringen.

Det stadig større omfanget av digitalisering både privat og på jobb, og at den private og profesjonelle hverdagen i stadig større grad smelter sammen, gir noen nye utfordringer. Sentralt er behovet for større bevissthet for hvilken rolle medarbeiderne til enhver tid har. Er det f.eks. greit å benytte arbeidsgivers digitale verktøy for privat aktivitet, og motsatt; er det greit å bruke privat digitalt utstyr til arbeidsrelaterte oppgaver. Spørsmålet er aktuelt siden graden av tekniske sikkerhet ofte er ulik. Muligheten for sikker elektronisk kommunikasjon og lagring er vanligvs nokså forskjellig. Materiale som er personsensitivt, eller sensitivt på annen måte, må vanligvis behandles i et sikkert fagsystem innenfor virksomhetens brannmurer for å kunne vurderes å være forsvarlig behandlet.

Ytterligere utfordringer oppstår når virksomheter tar i bruk sosiale medier som en del av informasjonsflyt og brukerdialog. Her er informasjonssikkerheten i alminnelighet ikke tilfredstillende, og et bevisst forhold til informasjonsflyten er nødvendig. Hvordan informasjonen flyter rent datateknisk er det de færreste gitt å overskue.

For å kunne navigere i et landskap hvor det private og det profesjonelle flyter sammen forutsettes en forståelse av hva som er personopplysninger f.eks. Behovet for kunnskap og verdiforankrede holdninger er tilstede, og internopplæring og formidling av organisasjonsverdier får stadig større betydning.

Den **statlige styringen** er en mål- og resultatstyring: "Mål- og resultatstyring er det grunnleggende styringsprinsippet i statlige virksomheter.» (Senter for statlig økonomistyring, 2014) I veilederen for mål- og resultatsturing sies det:

1.1 Hva er mål- og resultatstyring?

Mål- og resultatstyring kan defineres som følger:

Å sette mål for hva virksomheten skal oppnå, å måle resultater og sammenligne dem med målene, og bruke denne informasjonen til styring, kontroll og læring for å utvikle og forbedre virksomheten.

Dette forutsetter et styringssystem som er forankret i ledelsen, og som består av regelmessige, formelle prosesser. Et slikt system kan fremstilles som et hjul med gjensidig avhengige steg som følger etter hverandre i en syklus:

Figur 1.1 Styringshjulet

(Senter for statlig økonomistyring, 2014)

Det er en fare ved målstyring at det fastsettes målindikatorer, eller styringsparametere, som ikke fullt ut korrelerer med målet, og hvor adferden styres mot indikatoren og ikke mot målet. Hvilke indikatorer kan benyttes for å måle om organisasjonen ivaretar personvernet? Det angis at «resultater som ikke kan måles kvantitativt bør måles kvalitativt». (Senter for statlig økonomistyring, 2014) Det er imidlertid ofte lettere sagt enn gjort, og det er grunn for å tro at ofte ender man opp med «noe» som kan telles. Antall avvik og eventuelt hvor grove de er, kan være et alternativ. Gjennomførte risikovurderinger med indentifisering av uakseptable risikoer, kan være et annet. Men hvilken kunnskap gir risikovurderinger oss i realiteten?

Illustrasjon: Risiko måles gjerne som produktet av sannsynlighet og konsekvens, men hva er sannsynlig og hvordan gradere konsekvenser? Tilsvarende med gradering av avvik, - hva er grovere enn et annet? Og ikke minst hva er egentlig risiko, og hvordan forholder den enkelte seg til disse begrepene? Avhengig av om en vurderer risiko opp mot risikovilje eller risikoaversjon vil dette valget gi ganske ulike resultater. Det er vel også i alminnelighet slik at mennesker frykter «tap» mer enn de ønsker gevinster. Når så innholdet i begrepene risiko,

sannsynlighet og konsekvens er så uklart, hva gir så en risiko- analyse oss? Og ikke minst hva forteller det oss om vi teller hvor mange risiko-analyser som er gjennomført?

Når målindikatorene reflekterer graden av suksess, og når klassifiseringen i stor grad er subjektiv, hvor verdifull er målstyringen i en slik sammenheng? Og hvor etterrettelig er resultatet vi måler? Disse illustrasjonene viser etter mitt skjønn at mål- og resultatstyring kan ha betydelige svakheter når resultatet ikke uten videre kan angis i en relevant tallstørrelse. Dette drøftes videre under overskriften «individuelt nivå» nedenfor.

Det kan være grunnlag for å hevde at der verdien i resultatet er et viktigere element enn det som kan telles, vil det kreves mer institusjonelle virkemidler enn instrumentelle for å lykkes. Videre hevder Høyer (Høyer, upublisert) at jo større utfallsrom eller uforutsigbarhet det er i fokusområdet, jo «tykkere» institusjonell tilnærming er nødvendig.

Min hypotese baserer seg på at graden av instrumentell eller institusjonell tilnærming er en avgjørende faktor for hvor godt man lykkes med å ivareta personvernhensyn. Utgangspunktet for mye av den styringen som praktiseres er forutsetningen om at mennesket, og for så vidt organisasjoner, agerer rasjonelt. Det er stilt spørsmål om dette er en myte (Mach, 2008), og i så tilfelle, hva er det da som påvirker valg av handlingsalternativ istedenfor eller i tillegg til? Jeg kommer tilbake til dette nedenfor.

Etter min oppfatning er det grunnlag for å stille spørsmål ved statens ensidige forkus på mål- og resultatstyring. Det synes som eneste hensynet som er tatt for mål som er vanskelig å måle, er henvisningen til en kvalitativ måling i stedet for en kvantitativ. I samfunnsforskningen er det i alminnelighet en bevisst holdning til om man velger en kvalitativ eller kvantitativ forskningsmetode. Dette burde også reflekteres hos de som styrer samfunnet slik at styringen kan tilpasses også diffuse mål.

Nå skal jeg gå over til å diskutere hvordan den nasjonale styringen operasjonaliseres hos de informatene jeg har vært i kontakt med, og særlig i forhold til oppgaven med å sørge for at den enkelte har et godt personvern.

Datatilsynet

Datatilsynet ser opplagt utfordringen med å initiere etablering av personvern som verdi i organisasjonene i tillegg til etterlevelse av regelverket i lov og forskrift. Datatilsynet er både

tilsyn, ombud, vedtaksmyndighet og rådgiver. De er selvsagt likevel først og fremst et tilsyn som skal føre tilsyn med at reglene etterleves. Det er begrenset hvilke verktøy og hvilke ressurser de har for å drive det informasjons- og påvirkningsarbeid som er nødvendig for å sette fokus på annet enn etterlevelse. Selv om det skal bemerkes at de gjør en stor jobb også her. Det er vel heller overordnet myndighet som må bære ansvaret for at både tildelte ressurser og målstyringen både styrer og begrenser aktiviteten.

Tilsynet er også en statlig institusjon som er underlagt en mål og resultatstyring, og de blir nok målt på noe som kan måles. Datatilsynet, som de fleste andre statlige organisasjoner, mottar årlig et tildelingsbrev som er et styringsdokument for organisasjonene.

Tildelingsbrev er det sentrale styringsinstrumentet fra et departement til en underliggende virksomhet. Tildelingsbrevet skisserer økonomiske rammer og beskrivelser prioriteringer, resultatmål og rapporteringskrav for virksomhetene. Tildelingsbrevene sendes virksomhetene årlig etter behandlingen av statsbudsjettet i Stortinget. (Kommunal og moderniseringsdepartementet, 2014)

I tildelingsbrev til Datatilsynet for 2014 (Kommunal og moderniseringsdepartementet, 2014) heter det:

Hovedmålet på personvernområdet er at alle skal ha personvernbeskyttelse i tråd med gjeldende personopplysningsregelverk… hovedaktiviteter for å realisere hovedmålet:
- skape oppmerksomhet om behov for personvern og gjøre personvernspørsmål mer relevante i folks hverdag
- øke kjennskapen til lovfestede plikter og rettigheter både i befolkningen og i virksomheter
- fremme bruk av innebygd personvern og stimulere til at personvernhensyn blir tatt tidlig ved utvikling av nye løsninger eller nytt regelverk
- gjennomføre tilsyn i prioriterte sektorer basert på risikoanalyse, systematisere og kommunisere funn fra tilsynene til aktuelle målgrupper samt følge opp etterlevelse av pålegg
- delta aktivt i internasjonalt personvernarbeid

Videre kreves det av rapportering bl.a.:

> *Årsrapporten for 2014 skal gi et dekkende bilde av Datatilsynets resultater, og gi departementet grunnlag for å vurdere måloppnåelse og ressursbruk.*

Videre:

> *Datatilsynet [skal] redegjøre for prioriterte sektorer, samt valg og omfang av de ulike virkemidlene og tiltakene innenfor hver hovedaktivitet. Rapportering om*

> *tilsynsaktivitetene skal inneholde informasjon om antall gjennomførte tilsyn fordelt på sektorer og medgåtte ressurser i dette arbeidet.*

Dette er mine utklipp som ikke fullt ut yter oppdragsbrevet rettferdighet. Det reflekter likevel etter mitt skjønn en holdning om at det som ikke kan måles, har det mindre verdi.

De reglene Datatilsynet er satt til å forvalte er særlig instrumenntelle i sin utforming. Kravene i forskriften slik formulert at det er en plikt for å gjennomføre risikovurderinger, revisjoner og avviksbehandling. Og dette skal dokumenteres. Se f.eks. personopplysningsforskriftens kapittel 2. Dette er selvsagt lett å gripe fatt i på et tilsyn, men spørsmålet om systemet virker, eller bare skaper et skinn av kontroll, er ikke like lett å avklare. Det er stor forskjell på det å kontrollere, og det å ha kontroll. Det er enkelt å dokumentere en risikovurdering, men om den er gjennomført på en kvalifisert måte er betydelig mer krevende.

Under overordnede prioriteringer i tildelingsbrevet heter det:

> *Personvern er en ideell interesse. Det overordnede målet er å oppnå god ivaretakelse av personvernet i avveiningen mot andre samfunnsinteresser. Gjennom tilsyn og saksbehandling skal Datatilsynet kontrollere at lover og forskrifter om behandling av personopplysninger blir fulgt, og at feil og mangler rettes.* (Kommunal og moderniseringsdepartementet, 2014)

Som man ser er personvern beskrevet som en "ideell interesse". "Ideell" betyr rent språklig slik det er brukt her nærmest "som bygger etiske idealer". Etter mitt skjønn er dette i beste fall en misforståelse i forhold til slik personvernet er beskrevet både i gunnloven, av regjeringen overordnet og av Datatilsynet selv (se ovenfor side 7 og 8). Der er personvern tydelig beskrevet som en rettighet den enkelte har til et privatliv. Det fremstår som påfallende at individets rett til personvern ikke er reflektert i tildelingsbrevet. Det kan synes som departementet har sett seg blind på styringslogikken, og at fokus på regeletterlevelse er det mest sentrale. At den grunnleggende retten til personvern for den enkelte har glippet ut allerede i første operasjonalisering fra statens side, gir grunn for bekymring. Dette er i seg selv tilstrekkelig grunn for kritikk av mål- og resultatstyring av målsetninger som er lite målbare. Å oppfylle retten til personvern er en internasjonal forpliktelse, og som er gitt grunnlovsvern. Særlig mer forpliktende kan det neppe bli på nasjonalt nivå. Når dette mislykkes allerede fra departementets side i dette tilfelle, kan en spørre hvordan mindre forpliktende nasjonalpolitiske føringer implementeres i styringsdialogen.

Men det er ikke Datatilsynet som er en del av mitt empiriske grunnlag. De har hjulpet meg med gode refleksjoner for prosjektet, og er også sentrale i personvernarbeidet i Norge. Det synes som de langt på vei deler noen av de refleksjonene jeg har rundt utfordringer knyttet til mitt forskningsspørsmål.

De to statlige organisasjonene A og B

Disse organisasjonene blir som andre statlige organisasjoner styrt gjennom budsjett og tildelingsbrev i tillegg til relevant lovregulering, som for begge definerer formål med organisasjonene. Ingen av de to organisasjonene har i tildelingsbrevet får krav om å ivareta personvernet til tross for at de begge som nevnt behandler betydelige mengder personopplysninger. Den ene er imidlertid pålagt krav og rapportering om informasjonssikkerhet. Som vi husker er konfidensialitet en del av informasjonssikkerheten, og personvernet er ved det langt på vei også omfattet.

Imidlertid er selvsagt disse organisasjonene, som alle andre, forpliktet til å følge de lovreguleringene som vi har i Norge. Lovregulering kan ha mange ulike formål. Fordele rettigheter og goder, regulere forbud og plikter, for å nevne noen. Blant jussens oppaver er å styre sammfunnsmedlemmers adferd og samfunnsutviklingen i alminnelighet (Aubert, 1982). Det er derfor i noen grad relevant å trekke inn lov- og forskriftsregulering som en del av den statlige styringen. Ikke denne reguleringen som sådan, men deler av bestemmelsene vil ha styringsaspekter ved seg.

De kravene som er i blant annet Grunnloven og personopplysningsloven vil derved organisasjonene A og B være forpliktet til å operasjonalisere inn i sin drift. Begge har som jeg tidligere har redegjort for, implementert mange av bestemmelsene i personopplysningsloven med forskrift i sine interne styringsdokumenter. Ingen av dem opplyser om at det er noe særskilt fokus på å implementere det grunnlovsfestede kravet den enkelte har på personvern. De har imidlertid begge et stort fokus på å bygge og forvalte sitt eget omdømme. Dette sammen med bestrebelsene på å etterleve regelverket som Datatilsynet forvalter, synes å bidra til at konfidensialiteten overholdes rimelig godt.

Spørsmålet er da om det representerer noe problem dersom den enkelte faktisk oppnår et personvern? Slik jeg ser det vil dette etablere en annen verdi hos medarbeiderne enn det som er formålet i Grunnlovens § 102. Første ledd i bestemmelsen har “enhver” som subjekt, og det handler om retten til personvern. Paragrafens annet ledd har “Statens myndigheter” som

subjekt, og handler om å verne den enkeltes integritet. Her kan bemerkes at styringssignalet som gis i personopplysningsloven er riktig. Men når operasjonaliseringen av første ledd gir seg utslag i vern av eget omdømme, er subjektet endret. Fokuset er flyttet fra enhver borger til organisasjonens eget omdømme. Nå vil det trolig være slik at vern av egnet omdømme er en så sentral verdi for organisasjonens legitimitet, og ivaretagelse av personvernet vil være en del av denne, at mange vil mene at problemstillingen mest er av akademisk interesse. Jeg deler ikke denne oppfatningen.

Det kan f.eks. være slik at noen organisasjoner har et omdømme og en legitimitet i to retninger. Hvis vi tenker på det offentliges ulike pengeinnkrevere, vil de neppe etablere noe godt omdømme i forhold til de borgere som blir utsatt for tvangsinndrivelse av pengekravene. Legitimiteten og det gode omdømme etablerer de hos andre offentlige organisasjoner og hos lovlydige borgere med god betalingsevne. Personvernet til de som sliter med å betale sine forpliktelser vil da være uavhengig av organsiasjonens omdømme som bygges i forhold til andre aktører. Dette kan være et eksempel på at oppmerksomhetet på eget omdømme i seg selv ikke nødvendigvis er motivernede for å ivareta et godt personvern.

Det er derfor min påstand at bevissthet om at personvern er en rett for enkeltindividet er viktig for å etablere en "riktig" verdiforankring hos organisasjoners medarbeidere. Poenget er som nevnt over at verdien "personvern" har et annet subjekt enn verdien "omdømme".

Jeg skal i det videre drøfte styringsdialogen og rammene for å ivareta personvernet ut fra flere perspektiver, og vil starte med det overornede og bevege meg i retning av individet. Eller fra makro nivå til mikro nivå om man vil. De ulike aspektene vil søkes belyst underveis og knyttes til det empiriske og det teoretiske materialet jeg har valgt ut.

5.1 Nasjonalt – statlig nivå

Staten har det overordnede ansvaret for ivaretakelsen av personvern. Staten i denne sammenheng betyr storting og regjering. Det følger av internasjonale forpliktelser bl.a. i menneskerettskonvensjonen som fastslår at "enhver har rett til respekt for sitt privatliv…". Det er åpenbart at staten har dette ansvaret innenfor det som er statens anliggender. Like

selvsagt er at det stortinget som lovgivende myndighet må legge til rette for at personvern som en rettighet for enhver bestemmes som en forpliktelse.

Taushetsplikt av hensyn til borgerne eller brukerne, er imidlertid ikke noen nyhet. Taushetsplikt er som vi husker et utrykk for konfidensialitetskravet i personvernreglene. For prester i forbindelse med skriftemål har taushetsplikten en flere hudre år gammel historie. Om starten på denne formen for pliktig hemmelighold startet i kirken eller andre steder, er ikke poenget her. Det viser at personers krav på hemmelighold er en gammel tilnærming som i større eller mindre grad er en del av våre nedarvede forestillinger.

Personvern og taushetsplikt er ofte to sider av samme sak, men kan også i særlige tilfeller være motsetninger. Eksempler kan være der taushetsplikten hindrer at opplysninger om en planlagt forbrytelse gjøres kjent for noen som kan hindre det, eller hvor opplysninger fra barnevernet ikke tilflyter behandlingsapparatet slik at den mest adekvate behandlingen foretas. For en behandlingsinstitusjon for undom med traumer, vil opplysninger om et tidligere overgrep kunne bidra til en bedre behandling. Hva er det hensynet til den som har krav på personvern vil gi som det beste alternativet? Personvernet til overgriperen skal selvsagt også ivaretas, men det er ikke problematisk å få til.

Personvern er også en konsekvens av internasjonale forpliktelser, og regjeringen opplyser på sin hjemmeside (regjeringen, 2014) at disse ligger til grunn for den nasjonale personvernlovgivningen. Taushetsplikt er regulert i forvaltningsloven og en rekke andre lover, og har selvsagt en personvern side. Særlig kommer dette imidlertid til uttrykk i personopplysninglovens formålsbestemmelse som er gjengitt ovenfor. Den videre operasjonaliseringen av personvernet fra statlig side kommer til uttrykk på minst to måter:

1. Etablering av organisasjoner som skal bidra til å ivareta den enkeltes personvern. Her er to organisasjoner er sentrale:

    a. Norsk senter for informasjonssikring (NorSIS) er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. (Norsk senter for informasjonssikring, 2014) Deres oppdrag er: i) Bevisstgjøre om trusler og sårbarheter ii) Opplyse om konkrete tiltak gjennom nyheter, råd og veiledninger iii) Påvirke til gode holdninger innen informasjonssikkerhet. Nasjonal sikkerhetsmyndighet kan også nevnes i denne sammenheng. De har

et oppdrag som langt på vei ligner på NorSIS, men det er viere både i faglig tilnærming og i fokusområde. De dekker både sivil og militær sektor.

b. Datatilsynet er både tilsyn og ombud. Vi skal medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem. Datatilsynet er et uavhengig forvaltningsorgan administrativt underordnet Kongen og Kommunal- og moderniseringsdepartementet. (Datatilsynet, 2014)

2. Rettslig regulering hvor forpliktelsene kommer til uttrykk, særlig personopplysningsloven. Jeg avgrenser her mot lovregulering av taushetsplikt selv om slik regulering er en del av det totale bildet.

Regjeringen har ved dette etablert to organisasjoner hvor Datatilsynet i hovedsak er gitt tilsynsoppgaver, og NorSIS er gitt informasjons- og påvirkningsoppgaver. Sistnevnte synes å ha ett noe løsere definert oppdrag underlagt egne faglige vurderinger med sikte på å medvirke til at personvernet ivatetas av både private og offentlige organisasjoner samt imøtekomme innbyggernes behov. Styringssignalene er følgelig litt ulike. Det kan synes som NorSIS er gitt i oppdrag å forvalte den institusjonelle forståelsen, mens Datatilsynet gis som hovedoppgave å ivareta det instrumentelle perspektivet.

Når det gjelder Datatilsynet er den sentrale oppgaven å påse og kontrollere at personopplysningslovens regulering blir fulgt (jf. personopplysningsloven § 42). Lovens regulering består i hovedsak av noen handlingsplikter, eller vilkår om man vil, som må oppfylles for at personopplysninger lovlig kan behandles. Videre bestemmes hvordan organiseringen av informasjonssikkerhetsarbeidet skal være, og det kreves at alt dette er dokumentert.

Styringen av Datatilsynet og bestemmelsene om hvordan personvernet skal ivaretas, er utpreget instrumentelt i utformet. Det er krav om at de som skal behandle personopplysninger etablerer et system, og beskriver noen prosedyrer for å ivareta personvernet. Reguleringen er trolig utformet med sikte på å oppnå formålet med loven. Om disse bestemmelsene er tilstrekkelige eller formålstjenlige for å oppnå formålet i enhver situasjon, er ikke ytterligere reflektert i styringen. Datatilsynets tilsyn er rettet mot om lovens bestemmelser er oppfylt. Om et forsvarlig personvern er etablert i virksomheten, er ikke uten videre en del av det som skal kontrolleres. Datatilsynet opplyser i intervjuet at de alltid foretar intervjuer i tilknytning til

stedlige tilsyn. Formålet med intervjuene er blant annet å avdekke om informasjonssikkerhet er en verdi for virksomheten, eller om det bare er papirbestemmelser.

Spørsmålet blir så hvilken type styringssignaler er det staten gir til de som skal behandle personopplysninger, og til organisasjonen som skal føre tilsyn med dette? I forhold til Høyers (Høyer, upublisert) diskusjon rundt tynn og tykk institusjonalisme, må dette karakteriseres som en tynn institusjonell forståelse av oppgaven og det formål som søkes oppnådd. Tynn institusjonell tilnærming er i flg. Høyers drøftelse lite egnet for organisasjoner eller oppgaver hvor utfallsrommet er stort eller uforutsigbart bl.a. fordi et strengt regelregime kan hindre nødvendige spontane handlinger. Personvern og informasjonssikkerhet har etter mitt skjønn et stort utfallsrom, og med den digitaliseringen som pågår er det uforutsigbart hvilke trusler eller risikoer som kan oppstå. Det er derfor langt fra sikkert om statens instrumentelle styringssignaler er tilstekkelige for å møte hittil ukjente utfordringer for personvernet.

I boken Organisasjon og organisering (Busch, Vanebo, & Dehlin, 2010) reflekteres det over prosessen der en organisasjon blir en institusjon. I denne institusjonaliseringsprosessen splittes organisasjonen opp i to dimensjoner: rasjonelt verktøy og oganisk system (dette er behandlet i teorikapittelet). Det organiske systemet vil ta opp i seg de normer og verdier som er i omgivelsene, og etablere en forankring av disse verdiene i organisasjonen. Denne institusjonaliseringen hevdes å være viktigst for de organisasjoner som har diffuse mål, eller med mål som er lite målbare.

Verken Høyer (Høyer, upublisert) eller (Busch, Vanebo, & Dehlin, 2010) støtter den måten staten styrer Datatilsynet på spesielt, eller personvernet på mer generelt. Personvern som en verdi er nok likevel i noen, om enn varierende, grad implementert på overordnet statlig nivå uten at det drøftes videre her.

5.2 Organisasjons nivå

Jeg skal her først diskutere skillet mellom offentlige og private organisasjoner, og hvorfor det er av betydning. Deretter skal resultatene fra de to forskningskningarbeidene det er vist til tidligere, drøftes opp mot problemstillingen og funnene fra egne intervjuer.

Kravene til de som behandler personopplysninger er de samme enten oganisasjonen er privat eller offentlig. Offentlige organisasjoner behandler ofte mer personlige opplysninger. Eller for

å si det på en annen måte: De organisasjonene som behandler flest personopplysninger og også flest sensitive personopplysninger, er offentlige. Kravene til at offentlige organisasjoner skal opptre etterettelig og forvalte verdier som demokrati, åpenhet og personvern, er nok større enn forventningene til private organisasjoner. Jeg har tidligere avgrenset mitt tema til offentlige organisasjoner, og styringen av dem som en mulig variabel årsak til manglende måloppnåelse på personvernområdet.

Skillet privat- offentlig organisasjon

Det må først vurderes om det er noen ulikheter mellom privat og offentlig sektor som påvirker tilnærmingen. Det er nødvendig fordi krav og forventninger som nevnt er ulik. Her finnes det neppe noen klart ja/nei svar. Det må ses på hvilken type virksomhet som utøves. Det er flere eksempler på offentlige organisasjoner som driver foretningsmessig virkomhet, eller noe som ligner på det. På samme måten finnes det også noen særlige eksempler på private rettssubekter som utøver forvaltningsmyndighet. Det følger av dette at et skille mellom organiasjoner som utøver offentlig myndighet og andre kan være et utgangspunkt. Vi kan likevel ikke snevre det så mye inn. Da ville mye av offentlig tjenesteproduksjon falle utenfor. Den delen av denne produksjonen som har elementer av ikke-økonomiske verdier i seg, bør nok i forhold til temaet her betraktes som offentlig sektor. Dermed faller en del av den virksomhet som er «privatisert», eller drives etter slike prinsipper innenfor. Eksempler her kan være barnehage, ungdomsklubb og kulturskole.

Hva er det som er spesielt med offentlig sektor, og som er av betydning for sondringen her? Offentlig sekstor har et kollektivt formål, og handler grunnleggende på vegne av oss alle. Rettsikkerhet og likebehandling kan være betegnende stikkord her. Videre er forventningene knyttet til demokrati, åpenhet og innsyn, men også til effektivitet i offentlige organisasjoner. Effektiviteten er også knyttet til å oppnå verdiene demokrati og åpenhet på en formålstjenlig måte. Slike verdier kan neppe måles i kroner, og en annen tilnærming enn den vi finner i privat sekstor er nødvendig.

I privat sektor vil alt i prinsippet måles mot graden av oppnådd profitt, og slike ullne verdibaserte målsettinger som demokrati og åpenhet representerer bare en kostnad i en slik kontekst. Handlingsbetingelsene er således ulike, og i tillegg kommer også problemstillingen med «gratispassasjerer». Fellesskapet må i et land som vårt, bære kostnadene også for de som ikke evner å bidra. Eller for så vidt også de som lurer seg unna. Dette er typiske sammfunnskostnader som det ikke uten videre kan forventes at private vil bære.

Etablering av organisasjoner

Når vi nå har sett på en omtrentlig avgrensning av den delen av offentlig sektor som må vurderes særskilt, må vi se på hvordan organiseringen og arbeidsmetodikken i organisasjoner beskrives. Det kan ses på som:

1. En strøm av problemer. Hvilke utfordinger er det organisasjonen arbeider med.
2. En strøm av løsninger. Hvordan løses utfordringene, og hvilken kunnskap og hvilke teknikker brukes i arbeidet.
3. En strøm av deltakere. Hvem er et som deltar i arbeidet med å løse utfordringene, og hva kjennetegner disse.
4. En strøm av beslutningsmuligheter. Når og hvor løses problemene, og hvilke føringer er gitt for handlingsrommet.

Det å koble disse strømmene er et bilde på organisering. Og når organiseringen blir varig og med gitte rammebetingelser, har vi en organisasjon.

Så blir det neste spørsmålet hvorledes skal disse organisasjonene styres og hvilket handlingsrom skal de gis. Og hvem skal ha innflytelse til å gi disse styringssignalene og på hvilken måte. Grunnleggende utfører offentlige organisasjoner sitt oppdrag på vegne av borgerne, men en direkte demokratisk styring av den enkelte oganisasjon er selvsagt ikke mulig. Når vi har en demokratisk styreform må vi tenke at de signalene borgerne gir ved valg skal reflekteres videre i hvordan organiseringen og styringen av offentlig sektor gjøres. Her vil regjering/storting, eller de som er gitt oppdrag med gjennomføring, kunne velge mellom to prinsippielt ulike tilnærminger: Den instrumentelle eller den institusjonelle tilnærmingen for styring. De to skiller seg fra hverandre på en rekke måter. Det er selvsagt ikke noe enten/eller tilnærming, men heller spørsmål om i hvilken grad de styrende ser på organisasjonen og oppgaveporteføljen med en instrumentell forståelse, eller med en institusjonell forståelse.

Som jeg har redegjort for tidligere kan skillet beskrives slik at ved en instrumentell forståelse anses organisasjonen som et verktøy som kan løse sine oppgaver nærmest uavhengig av hvilke mennesker som arbeider der og hvilke verdier de er bærere av. I den institusjonelle forståelsen ses organisasjonen som et organisk system hvor løsning av oppgavene forutsetter verdiorienterte medarbeiderne som også kan handle spontant der det er nødvendig (Høyer, upublisert).

Styringens funksjon

Den statlige styringen treffer også den enkelte organisasjon både direkte og av Datatilsynets påvirknings og tilsynsvirksomhet. Det overordnede målet som er relevant for dette forskningsarbeidet, er å sikre den enkeltes krav på personvern.

Er den styringen, og de insentiver og sanksjoner som staten benytter egnet til å oppnå formålet?

Den intrumentelle styringen og de virkemidlene og sanksjonene som er gitt, er gjennomgått tidligere. Jeg skal nå se om teori, annen forskning og mitt empiriske materiale gir støtte til de rammebetingelsene som er gitt for å ivareta personvernet.

Ut fra litteraturstudier synes å være en relativt utbredt oppfatning eller observasjon, i samfunnsvitenskapen at de strukturelle elementene som planer, instrukser og reglementer, ofte er løst koblet til hvilke aktiviteter som faktisk utføres. (Eriksson-Zetterquist, Kalling, & Alexander, 2012). Ofte brytes regler, og de enkelte handlingsvalg fører ikke alltid til ønsket resultat. De metoder eller prosedyrer som er bestemt, og kontroll av lojalitet til reglene, er utilstrekkelige for å oppnå de ønskede resultatene. Likevel er forestillingen om en rasjonalitet i oppgaveutførelsen en almen vurdering i organisasjonene. Det er langt på vei en institusjonalisert myte som tas for gitt. En nærliggende konklusjonen en kan rrekke ut av dette er at regler virker ikke alene.

Høyer (Høyer, upublisert) argumenterer for at den optimale styringen oppnås ved at både de styrende og de styrte har en tykk institusjonell forståelse av organisasjonen. For å gjennomføre tiltak, eller oppnå en tilstand, som er lite målbar, krever det i større grad en annen dynamikk i forholdet mellom tillit og kontroll enn det som er tilfellet ved en mer samlebåndslignende aktiviteter. Om en organisasjon er god til å ivareta personvernet er vanskelig å måle. Det som kan måles er hvilke aktiviteter og instruker som organisasjonen har og og rent faktisk gjenomfører. En kontroll, eller et tilsyn, av dokumentasjonen for at aktiviteter er foretatt og instrukser er på plass, vil i Høyers logikk resultere i at tilliten oppnås som en følge av kontrollen. Men hvilken tillit er det da som skapes? Det må jo være tilliten til at de intrumentelle kravene er oppfylt, men det gir neppe uten videre grunn for å ha tillit til at personvern er etablert som en tilstand. Personvernet utfordres på stadig nye måter og en dynamisk tilnærming til utfordringene er etter mitt skjønn nødvendig. Høyer argumenterer for at spontanitet vil være nødvendig for å kunne velge riktig handlingsalternativ i situasjoner som

rutinebeskrivelser ikke har tatt høyde for. Spontanitet fordrer en tillit fra de styrende til at den enkelte velger riktig handlingsalternativ, og så kommer oppfatningen av kontroll som en følge av den utviste tillit.

Tilsvarende tilnærming hadde Selznick (Selznick, 1957) som hevdet at å se på en organisasjon som både et rasjonelt verktøy og et organsisk system ville skape en "riktig" verdiforankring i organsisasjonen. Denne øvelsen anså ham som særlig viktig for de organisasjoner som har diffuse mål, eller mål som er lite målbare. For mer klare produksjonsmål eller annet, kan regler være en nødvendig forutsetning. Disse utsagnene må i noen grad tolkes i lys av den tiden teorien ble utviklet hvor den hieraktisk byråkratimodellen var den herskende styringsformen.

March (Mach, Fornuft og forandring, 1995, 2. utgave 2008) stiller også spørsmålet om rasjonalitet er en myte. Han diskuterer myten utfra ulike tilnærminger, og også utfra et åndelig grunnlag for lovprising av menneskeheten. Dersom man ser på mennesket som nyttemaksimerende så vil det i en økonomisk virkelighet kunne kalles grådig. I en markedsøkominsk kontekst vil det imidlertid forventes som en rasjonell tilnærming. Inn i en prinispal – agent-teori (Idsø) vil det være en naturlig konsekvens av en intrumentell forståelse av organisasjonen. Dette viser at det er ulike tilnærminger eller perspektiver for rasjonalitet, som kan gi ulik forståelse.

Dersom man i steden ser på mennesket som noe som ønsker å gjøre det gode, eller det riktige, kan en instumentell forståelse av organisasjonen gi feil signaler. "Inden for Kierkegaards og Quixotes forestillingeverden bliver handling først riktig menneskelig, når den ikke er redfærdiggort som noget intrumentelt." (Mach, Fornuft og forandring, 2008). Jeg tolker dette sitatet slik at handlinger bare kan sies å være forankret i et menneskes verdigrunnlag der de kan forklares med noe annet enn bare det at handlingsvalget fulgte av regler.

I den logikken som dagens statlige styring har vil det være rasjonelt for organisasjonene å oppfylle de kravene som settes, og som eventuelt kontrolleres. Om det er et objektivt rasjonelt handlingsvalg i det enkelte konkrete tilfellet i den praktiske virkelighet, vil ikke dette regime stille spørsmål ved. Dersom en annen og mer spontan aktivitet ville gitt en bedre ivaretakelse av personvernet, vil det kunne ha en kostnad siden det er i strid med reglene eller instruksen. Og hvis det er kostnader ved å handle rasjonelt, vil det være rasjonelt å ikke gjøre det. Det vil si at dersom styringssignalene er "feil", vil de fleste likevel følge dem fordi alternative handlinger resulterer i et avvik.

Nils Brunsson (Brunson, 2006) er opptatt av betydningen av å opprettholde drømmen om en rasjonell organisasjon, og at dette har en egenverdi. Han reflekterer, som flere andre forfattere som er nevnt, over den realitet at fullstendig rasjonell opptreden ikke er mulig på grunn av kapasitetsbegrensninger. Den enkelte medarbeider vil ikke i et hvert tilfelle kunne forholde seg til alle mulige utfall av et handlingsalternativ, og heller ikke overskue alle mulige ulike alternativ for handling eller aksjon.

Organisasjoner vil et styring – kontroll perspektiv operere på to nivåer: i) Et **handlingsnivå** hvor man håndterer ulike situasjoner i henhold til de verdier og/eller de regler og rutiner en organisasjon har. Eller ii) et **fortolkningsnivå** hvor man ofte reflekterer seg frem til at handlingene var utslag av et rasjonelt valg. Grunnen til det er at mennesker i en referanseramme der rasjonalitet er en verdi, vil ønske å handle rasjonelt. Og det å ikke handle i henhold til sin vilje, vil anses som nærmest syndig. Selv om det skulle foreligge en refleksjon om at feil ikke blir korrigert, eller probemer ikke blir løst, vil en lett ty til en hyklerisk omfavnelse av rasjonaliteten.

Så lenge rasjonaliteten framstår som et ideale, vil det forbli en ledestjerne. Håpet om å oppnå rasjonell adferd vil således være noe ønskelig selv om det ikke er realistisk. Og håp er en positiv følelse og anses nærmest som normal i sammenligning med fravær av håp. Håpet er således nødvendig, og en bærende kraft for forestillingen om at vi kan endre ting i en positiv retning.

En virkelig rasjonell person vil ha mindre håp, og være mindre håpefull enn de fleste. Dette kan beskrives på samme måte som forholdet mellom realisme og depresjon. På denne måten vil det å leve normen for rasjonalitet gjøre det vanskelig å beholde håpet. Bunsson stiller spørsmål om det kan være slik at dersom vi skal tro på en rasjonalitet i fremtiden, forutsetter det at vi ikke er rasjonelle nå?

Slik jeg oppfatter Brunsson vil håpet om å kunne oppnå en rasjonell organisering i fremtiden ha en verdi nærmest som en motivasjonsfaktor. I relasjon til den optimale strukturen og organiseringen av informasjonssikkerhetsarbeidet som regjeringen pålegger organisasjoner, vil håpet om å oppnå dette være en drivkraft og et mål. Forutsetningen må vel være at lovkravene fra staten oppfattes som rasjonelle eller formålstjenlige. Det er tidligere redegjort for at få fullt ut makter å innfri disse kravene, men at mange likevel oppnår en god oppfyllelse av verdien personvern. Spørsmålet er da om kravene oppfattes som rasjonelle. Dersom

kravene ikke vurderes som formålstjenlige eller rasjonelle, vil de ikke kunne etablere noe håp som en drivkraft for å oppnå en rasjonell organisasjon i fremtiden heller. Når det er slik at verdien personvern som er forankret blant annet i Grunnloven, er operasjonalisert til et pålegg om å etablere et system for å sikre informasjonssikkerhet i organisasjonene, er det beste en kan håpe på å unngå merknader på et tilsyn.

Annen forskning

Det er to andre forskningsarbeider jeg har tatt med meg som grunnlag for diskusjonen her. Både den fra Texas og den norske peker på hvilke utfordringer som er identifisert og som bør drøftes, eller vies oppmerksomhet for å få på plass et best mulig personvern.

Den norske undersøkelsen (Tranvik, 02/12) retter fokuset mot personopplysningsloven med forskrift, og studerer hvordan den kommunale regeletterlevelsen er i forhold til disse reglene spesielt. Den viser med andre ord hvordan styringen fungerer i praksis. Jeg skal nå drøfte rapportens funn opp mot mine funn.

Det presiseres at analysene dermed ikke er representative for kommunal regeletterlevelse i alminnelighet. Datatilsynets 86 rapporter fra tilsyn i kommunesektoren i perioden 2001 til 2008 ble analysert. Der var det brudd på reglene i 90 % av tilfellene, og i gjenomsnitt omlag fire vedtak per kontroll. Tranvik legger etter dette til grunn at regeletterlevelse ikke er en ubetydelig utfordring for disse kommunene.

Begrepet "etterlevelsesillusjon" lanseres, og det betegner situasjonen der overholdelse av lov og forskrift helt eller delvis er tilsynelatende. I praksis vil det bety at praktiseringen av reglene har et "offentlig ansikt" som ikke nødvendigvis reflekterer hvilken praksis organisasjonen i virkeligheten har. Effekten av dette er at omgivelsene får en positiv oppfatning av en lovlydig organsisasjon uten at den behøver å bære de kostnadene en virkelig regeletterlevelse innebærer.

I følge Tranvik (Tranvik, 02/12) er det **tre betingelser** som må være til stede for at etterlevelsesillusjon oppstår. For det første forutsettes det at organisasjonene har kunnskap om reglene, og i noen grad en vilje til å etterleve det. At kommunene har kunnskap om reglene er dokumentert i Tranviks arbeide (Tranvik, 02/12). Det samme uttaler Datatilsynet i kommuneundersøkelsen (Datatilsynet, 2014): "Datatilsynet mener det er tydelig at problemet med etterlevelse av regelverket skyldes prioriteringer og mangel på kompetanse heller enn manglende kjennskap til regelverket. Problemet skyldes derfor ikke mangel på informasjon.»

I samme undersøkelse (Datatilsynet, 2014) er det klarlagt at et stort antall gir uttrykk for en vilje til å etteleve regelverket, men at kompetanse og kapasitet er barrierer i dette arbeidet. Datatilsynet analyserer det også slik at større kommuner ofte er bedre enn mindre kommuner. Det er derfor ikke overraskende at de to statlige organisasjonene A og B har god kjennskap til regelverket, og en uttrykt vilje til å etterleve det.

Den **andre betingelsen** som må være oppfylt er at viljen til å følge regelverket er større enn evnen til faktisk å gjøre det. Datatilsynets kommuneundersøkelse (Datatilsynet, 2014) viser at viljen ofte er tilstede, men mange viser til at de mangler både kompetanse og ressurser til faktisk å gjøre det. Den andre betingelsen synes med det langt på vei å være på plass for mange kommuner i Datatilsynets kommuneundersøkelse. Tranviks undersøkelse (Tranvik, 02/12) problematiserer evnen til å følge reglene ytterligere. I kommunenen er det rådmannen som har det formelle ansvaret, mens det praktiske arbeidet oftest ligger hos andre. De med det praktiske ansvaret beskrev utfordringer med å «markedsføre» regelverket overfor rådmannen. Tilsynsbesøk førte til større fokus hos rådmannen, med det hevdes at dette økte fokuset var av relativt kortvarig karakter. Enkelte hevdet også at det økte fokuset hos toppleder ga seg utslag i budsjettering av sikkerhetsarbeidet og at rådmannen på den måten kjøpte seg ut av den praktiske styringen og ansvaret.

De fleste kommunene som var med i undersøkelsen hadde laget risikovurderinger, men slike ble i liten grad vektlagt i det videre arbeidet fordi den ofte var laget på et underordnet nivå. Noen sanksjoner eller andre virkemidler for å følge opp pålegg internt i organisasjonene var ikke tilstede, og flere som arbeidet med sikkerheten opplevde å sitte med ansvaret for noe som toppleder har det juridiske ansvaret for. Dette viser at det å implementere et instrumentelt regelverk i organisasjonen uten et internt styringsregime som evner å følge det opp, er utfordrende å få til.

Det samme kommer også til syne ved at mange av sikkerhetslederne ønsket en overordnet styring som ga støtte til deres arbeid, men ikke en styring som begrenset deres selvstendighet i valg av virkemidler og handlinger. Slik jeg ser det viser dette at den instrumentelle overordnede styringen implementeres til organisasjonsnivå, og det er ikke lett å unngå slik reglene er utformet. Men tilnærmingen fra de som gjør jobben er at de ønsker lederstøtte og budsjett, men ikke at styringen begrenser selvstendighet i oppgaveutførelsen. Slik det er beskrevet i undersøkelsen kan det tolkes slik at de som utfører oppgaven etterspør bred tillit ved løsning av oppgaven, mens styringen er preget av krav til etablering av regler og rutiner.

I Høyers logikk (Høyer, upublisert) er dette en klassisk situasjon hvor styringen er preget av tynn institusjonalisme, mens den styrte etterspør tykk institusjonalisme. I følge Høyer er det beste at både de styrte og de styrende har samme forståelse, og helst en tykk institusjonell forståelse. Forholdet og dynamikken mellom tillit og kontroll blir krevende der den institusjonelle forståelsen er ulik hos de styrende og de styrte. Uansett er det i forhold til mange kommuner dokumentert at viljen er større enn evnen til å etterleve reglene, og andre betingelse er derved oppfylt for disse.

Hvordan er det så med de to statlige organisasjonene i mitt empiriske materiale? Er viljen større enn evnen til regeletterlevelse også der? Viljen er åpenbart tilstede og forankret på ledernivå i begge organisasjonene.

Organisasjon A har utfordringer med at informasjonssikkerhetsarbeidet er en relativt ny øvelse når det gjelder systematisk tilnærming og etablering av personvernombud. Evnen er derved noe begrenset siden det systematiske arbeidet ikke er ferdigstilt. Organisasjonen har også en utfordring med den desentraliserte strukturen, og at styringssignalene innenfra og ut må gå gjennom topplededelsen både sentralt og desentralt. Dette innebærer en streng hierarkisk styring hvor det synes som ingen har fullmakt til å gi styringssignaler direkte til noen medarbeidere ute.

Organisasjon A har slik jeg ser det dermed begrenset evne til å etterleve reglene på to fronter; både på kapasitet/kompetanse og styringsmessig. Dette indikerer at viljen er større en evnen i denne organisasjonen.

Orgaisasjon B har oppfylt mange av kravene i reglene allerede. Eneste utfordringen kan være at tilnærmingen er bredere ved at de ser på sikkerhet i et større perspektiv enn bare informasjonssikkerhet. Det er ingen indikasjoner på at det reduserer evnen, men kan påvirke prioriteringene. Informanten oppgir også et ønske om ytterligere kapasitet for å arbeide med personvern og informasjonssikkerhet. Dette kan like gjerne vitne om personlig engasjement og ønske om å gjøre det beste, som for liten evne i organisasjonen som sådan. Det er i hvert fall ingen klare indikasjoner på en ubalanse mellom vilje og evne i organisasjon B.

Den **tredje betingelsen** for at en etterlevelsesillusjon kan oppstå, er at det er mulig å skjule reell regelpraksis (Tranvik, 02/12). Dette punktet er relatert til regelutformingen og dokumentasjonsplikten som er oppstilt der. Det er derfor viktig for de organisasjonenen som håndterer personopplysninger at de lager og vedlikeholder slik dokmentasjon. I Tranviks

rapport er det dokumentert at 17 av 19 kommuner hadde laget mesteparten av dokumentasjonen som kreves. Likevel oppga mange i intervjuene at det var liten sammenheng mellom det som dokumentene viste og hva kommunene faktisk gjorde. Datatilsynets kontrollrapporter viste også ofte til at kommunenen ikke hadde gjort bruk av egne rutiner i det praktiske arbeidet.

Det antydes at mange kommuner hadde søkt opp andres dokumentasjon, og veiledninger hos Datatilsynet, for å nærmest kopiere dette inn som sitt eget. Det er også slik at underskelsen viste at mange av de 19 kommunenen hadde svært lik dokumenasjon.

Årsaken til dette kan være både utstrakt kopiering, men også at bruk av konsulenter med et standarisert opplegg, kan gi samme resultat. Det er også et spørsmål om regelverket i seg selv sammen med Datatilsynets maler og veiledninger også kan ha som resultat stor likhet i dokumentasjonen. Uansett er poenget at reglene gir mulighet for dokumentere etterlevelse uten at det nødvendigvis reflekterer realiteten. Den likheten som er dokumentert leder også tanken mot temaet isomorfisme. Mer om isomorfisme og fordeler og utfordringer med det i eget avsnitt nedenfor.

Diskusjonen over er relatert til kommuner, men jeg har også relatert til de intervjuene jeg har foretatt. Når det gjelder muligheten for å skjule praksis ved å lage dokumenasjon, vil det være felles for alle organisasjoner. I organisasjonene A og B er det få indikasjoner på dette, men begge opplyser at de har etablert et system for avvikshåndtering, men sliter med å få det til å fungere slik det skal. Årsaken synes å ligge i organisasjonen eller kanskje snarere i organisasjonens medlemmer. Mer om dette under kapittelet «individuelt nivå».

Samlet er det grunnlag for å hevde at muligheten for å skape en etterlevelsesillusjon er tilstede generelt slik krav, styring og kontroll er etablert fra sentrale myndigheter, og slik det derved i stor grad blir implementert på organisasjonsnivå.

Så langt er det grunn for å hevde at min hypotese om at mer institusjonell tilnærming gir bedre personvern, er styrket.

Undersøkelsen fra Texas tar utgangspunkt i litteraturstudier for å identifisere de mest vanlige faktorene som anses viktige for informasjonssikkerheten. Det ble indentifisert seks faktorer som anses viktige for god informasjonssikkerhet, men mye av litteraturgrunnlaget er fra privat

sektor. Undersøkelsen tar sikte på å avdekke om det som hevdes i litteraturen også gjelder for offentlig sektor. Det legges til grunn at offentlig sektor har mer ambisiøse mål enn de private organisasjonene med hensyn til informasjonssikkerhet, og at de har større ressurser. Det reflekteres også over at de ulike organisasjonene har ulik kultur som en følge av hvor ambisiøse målene er.

Undersøkelsen er en kvantitativ spørreundersøkelse som ble sendt alle statlige byråer i Texas. Det var en svarprosent på 38,5 på organisasjonsnivå, men det argumenteres for at undersøkelsen likevel er representativ siden det var flest svar fra de største organisasjonene. Hvis en ser på antallet medarbeidere som er representert i undersøkelsen, anses den likevel for å gi et dekkende bilde.

Undersøkelsen redegjør for resultatene i forhold til alle seks undersøkte faktorer. Jeg skal ikke her bringe inn mer fra undersøkelsen enn det som er relevant for diskusjonen om styringen. Det konkluderes med at støtte fra øverste ledelse har stor betydning for hvor god informasjonssikkerhet det er i den enkelte organisasjon. Lederstøtte har direkte betydning for fem av faktorene. Når det gjelder årsakene for brudd på informasjonssikkerheten, som er faktoren nummer seks, ga undersøkelsen ett resultat som kan illustreres og rangeres slik:

1. Sluttbrukerfeil
2. Hacker angrep
3. Manglende kompetanse hos medarbeiderene
4. Manglende trening av medarbeiderene

Det er betegnende at tre av topp fire årsaker til informasjonssikkerhetshendelser, er relatert til medarbeiderne.

Det er lite å finne rundt kompetanseoppbygging og trening av medarbeidere i de styringssignalene som gis fra nasjonalt nivå. Det betyr at denne tilnærmingen for en stor del er overlatt til den enkelte organisasjon å reflektere over, og å implementere i sin egen tilnærming til temaet. Både de undersøkelsene som er vist til over, og i intervjuene av organisasjonenen A og B, fremkommer det at kravene om system og dokumentasjon i personopplysningsloven med forskrift, er arbeidskrevende å få på plass. Det er grunn for å tro at dette likevel vil bli prioritert. Dersom man i tillegg skal sette av tid og øvrige ressurser i

form av opplæring på temaet personvern, er det enda vanskeligere å finne rom for en slik prioritering.

Både organisasjon A og B viser til at informasjonssikkerhet er tema ved opplæring av nye ansatte. For øvrig er det få signaler om et strategisk fokus på kompetanseoppbygging av medarbeiderne på dette temaet. Det vises til at motivasjon og påminnelser om at personvern er viktig, og i begge organisasjonene synes det å være forankret i at organisasjonens omdømme må tas vare på.

Sett i kontekst med undersøkelsen fra Texas er det påfallende at styringssignalene ikke dreies mot krav om opplæringsprogram som alternativ til noen av de andre kravene om systemer og dokumentasjon. Eller med andre ord en dreining mot en mer institusjonelt tilnærming til de utfordringene som ligger i å etablere et godt personvern. Den økte oppmerksomheten mot etablering av personvernombud, kan bringe utviklingen i en slik retning.

Isomorfi

Isomorfisk betyr rent språklig "samme form". Her skal jeg diskutere årsaker og mulige utfordringer ved den likhet som skapt, eller ønskes skapt.

Den diskusjonen som er foretatt over viser at det på informasjonssikkerhetsområdet er flere utslag av isoformisme. Det er ikke noe suspekt i det, men bare et utslag av at flere av kanskje ulike grunner, har endt opp med samme løsninger. I alminnelighet er det ansett som både positivt og effektivt å lære av hverandre, og også dele sine egne løsninger med andre. På den annen side er det også eksempler på at innføring av noe som har vært en suksess et sted, ikke alltid gir samme resultet et annet sted. Omgivelser og rammebetingelser er ofte ulike, og det må også med i vurderingene før en kopierer et system eller en fremgansmåte. I Tranviks undersøkelse (Tranvik, 02/12) er det vist til at mange synes å kopiere bl.a. systembeskrivelser fra andre, men uten at de reflekterer noen realitet. Få vil anerkjenne det som en positiv form for isomorfi.

I organisasjonsteorien skilles det gjerne på flere former for isoformi etter hva som er bakgrunnen for at likhet oppstår. Det skilles på tvungen, mimetisk og normativ isomorfisme. (DiMaggio & Powell, 1991) Disse er ikke inbyrdes eksluderende, men kan opptre samtidig.

Tvungen isomorfisme er gjerne et utslag av politisk påvirkning. Dette kommer i ytterste konsekvens til uttrykk gjennom lovregulering, men også på andre måter og via andre

styringssignaler. For temaet informasjonssikkerhet og personvern kommer det tydeligst til uttrykk i personopplysningsloven med forskrift. Disse reglene pålegger de som behandler personopplysninger å innføre nærmere bestemte prosedyrer, systemer og krav til dokumentasjon. Vi får tro at dette er bestemt i beste mening, og med sikte på å etablere et godt personvern. Noe av dette er diskutert tidligere, og viser at det ikke alltid er resultatet. Det gir vel tvert i mot grunn for beskymring for om formålet med personopplysningsloven vil oppnås slik det er regulert nå. Dette bør gi grunn for å revurdere både reguleringen og virkemiddelbruken. På et område som personvern med stort utfallsrom og stor usikkerhet kan det være grunn for å vurdere Høyers (Høyer, upublisert) tilnærming om at både de styrende og de styrte bør ha en tykk institusjonell forståelse av organisasjonen. Dette får de ikke ved dagens styringsregime.

Når det gjelder styringen på nasjonalt nivå er den underlagt en mål- og resultatstyring. Dette påvirker blant annet hvordan Datatilsynets løser sitt samfunnsoppdrag. Dette vil igjen påvirke hvilket fokus den enkelte organisasjon har ved ivaretakelsen av personvernet. Her er det grunn for hevde at en normativ isoformisme påføres organisasjonene både via rettsregler, men også via sentrale myndigheters påvirkningarbeide og tilsynsaktivitet.

Mimetisk isoformisme kan ofte være et utslag av usikkerhet. Mimetisk i denne sammenhengen betyr det samme som imiterende. Som tidligere nevnt er deling av kunnskap, og læring av hverandre, ofte en god tilnærming. Når en organisasjon skal implementere personopplysningslovens krav, vil det kreve at en setter seg inn i bestemmelsene og forstår hva som kreves. Dette kan for noen være vanskelig tilgjengelig, og da kan en løsning være å imitere det andre har gjort. Tranvik (Tranvik, 02/12) viser til at slik imitering eller kopiering er gjort i flere tilfeller. Om det er et utslag av usikkerhet, manglende selvtillit, manglende kapasitet eller av ren latskap, er ikke uten videre klart. Uansett er resultatet at her er det i realiteten misforholdet mellom vilje og evne til å etterleve regelverket som er imitert. Det er i hvert fall ikke særlig fortjenestesfullt, og er et eksempel på et uheldig utslag av mimetisk isoformisme.

Normativ isoformisme kommer som regel ut fra en profesjonalisering. De fleste ansatte, i hvert fall i ledende stillinger, har en balast i sin utdannelse. De vil da ta med seg den kunnskapen og de holdninger som utdannelsen har skapt inn i sin yrkesutøvelse. Ansatte med lik utdannelse vil et stykke på vei ha en lik tilnærming og forståelse, og løsningen av oppgaver vil være preget av disse erfaringene og den kompetansen men har tilegnet seg. Inn i arbeidet

med personvern vil dette påvirke tenkesettet og hvilke innrettninger som etableres. På **nasjonalt nivå** er Senter for statlig økonomistyring gitt ansvaret for å utforme den statlige styringen generelt. Det er grunn for å anta at medarbeiderene der er preget av en økonomisk tenkning i styringslogikken. Økonomistyring er nødvendigvis instrumentell i formen, i hvert fall på et operativt nivå. Det er trolig liten plass for "tykk institusjonell forståelse" (Høyer, upublisert) i denne konteksten. Dette preger også den styringen, og de mål og indikatorer som formidles i forhold til ikke målbare mål. Se f.eks. tildelingsbrevtet til Datatilsynet (Kommunal og moderniseringsdepartementet, 2014).

På **organisasjons nivå** vil hvilken utdanningsbakgrunn medarbeidere med ansvar for informasjonssikkerhet har, påvirke hvordan oppgavene blir løst. En økonom eller en revisor vil ha en annen referanseramme enn en statsviter eller en jurist. Både organisasjon A og B har jurister som personvernombud. I følge Datatilsynet er disse to organisasjonene blant de som lykkes best med informasjonssikkerheten. En av de opplyser at de fleste andre personvernombudene er tilknyttet organisasjonenes HR- avdelinger, uten at utdanningsbakgrunn er kjent. En kan ikke herfra trekke noen konklusjon om at jurister er best egnet til å ivateta informasjonssikkerhetsarbeidet. Poenget er at hvem man rekrutterer for oppgaven eller tildeler ansvaret, er av betydning. Det bør derfor være et bevisst valg slik at rett person får ansvaret.

Det er over diskutert både fordeler og ulemper ved ulike former for isofomisme. På informasjonssikkerhetsområdet er alle tre formene for isoformisme aktuelle og tilstede. Det er grunn for å være seg bevisst disse mekanismene, slik at uheldige utslag kan unngås. En slik refleksjonen synes i stor grad å være fraværende både på nasjonalt nivå og hos mange organisasjoner.

Det er **to andre dimensjoner**, eller andre tilnærminger, som også bør vies noe oppmerksomhet. For det første vil en slik ensartethet som isoformisme fører til også kunne kalles **konformitet**. Det kan da være grunn til å minne om at konformitet er den mest vanlige begrunnelsen for korrupsjon (Øverenget, 2013) i en presentasjon på Losby gods. 'Alle andre gjør det så da må det være greit at jeg gjør det også.' Selv om det ikke er korrupsjon å kopiere andres utjenlige informasjonssikkerhetsopplegg, vil "alle andre gjør det" argumentet kunne være en sovepute som hindrer egne vurderinger av om det tjener formålet.

Den andre dimensjonen er **endringsvilje**. Den homogeniseringen som isoformisme fører til kan skape en oppfatning av at det er slik rasjonelle, gjennomtenkte organisasjoner med høy legitimitet gjør. Tersklen for å foreta endringer blir da høy fordi det bryter med en mer eller mindre generell norm. På et område som personvern vil utfordringene endre seg, og ofte i et høyt tempo blant annet som følge av økende digitalisering. Behovet for endringer i takt med den dynamiske virkeligheten rundt oss, er nødvendig. Utfordringene kan være ulike i de mange organisasjonene som behandler personopplysninger, og en enhetlig struktur hos mange organisasjoner, kan være hemmende for nødvendige endringer.

Alle organisasjoner vil måtte forholde seg til den tvungne isomorfismen de utsettes for gjennom rettsreglene. Ytterligere refleksjoner fra både departementet (Kommunal og moderniseringsdepartementet, 2014) og fra Datatilsynet (Datatilsynet, 2014) om at etablering av personvernombud er en lur vei å gå, vil påvirke til ytterligere isomorfisme. Særlig vil dette gjelde dersom det blir en del av kravene i lov eller forskrift. Krav om personvernombud kan etter mitt skjønn få både positive og negative effekter. Et personvernombud vil kunne arbeide mer med å etablere verdien personvern i organisasjonen, og det er bra. Samtidig vil ytterligere krav som treffer alle som behandler personopplysninger, øke isomorfismen eller homogeniseringen enda ett hakk. Det kan ha som følge redusert endringsvilje eller evne, og det er ikke bra på et tema som er kontinuerlig i endring.

Uansett vil det være ett skritt i retning av en mer institusjonell forståelse, og da er det også opp til organisasjonene selv å styre aktiviteten til personvernombudet slik at verdien personvern etableres.

5.3 Individuelt nivå

Her skal jeg diskutere betydningen av enkeltindividers kompetanse og verdier som grunnlag for handlingsvalg.

”Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsadferd” Nasjonal sikkerhetsmyndighets definisjon av sikkerhetskultur (Najonal sikkerhetsmyndighet, 2013)

Denne definisjonen sier rett og slett at personvern til syvende og sist er en individuell øvelse. For å lykkes med personvern må den enkelte medarbeider aktiviseres og tilføres kunnskap slik at han eller hun utøver ønsket adferd.

Det er grunn for å ta Nasjonal sikkerhetsmyndighets definisjon på alvor. Selv om denne myndigheten har en bred arbeidsflate mot både sivil og militær sektor, anser jeg denne definisjonen for å være gyldig også på informasjonssikkerhetsområdet.

Det er ikke bare Nasjonal sikkerhetsmyndighet som ser betydningen av enkelt mennesket. Jeg vil sitere fra Gjørv- rapporten (Gjørv, 2012):

«Risikoen forstås og ansvaret plasseres på det intellektuelle plan, men det skjer ikke en dypere erkjennelse som gjør at de ansvarlige faktisk opplever å ha ansvar og at de har vilje og evne til å gjennomføre det man faktisk har bestemt seg for».

Alexandra Beck Gjørv

Leder 22-juli kommisjonen

Som man ser er betydningen til det enkelte individ vurdert som avgjørende i atskillig mer krevende situasjoner enn «bare» ved ivaretakelse av personvernet. Det ligger i kritikken av håndteringen av 22. juli hendelsen, og for så vidt også krigsoppgjøret etter 2. verdenskrig, at det kreves at det enkelte mennesket handler «riktig». I noen tilfeller har man en beredskapsplan for ekstreme situasjoner, og da er det viktig at denne er kjent og at den følges. Det kan likevel tenkes at det oppstår situasjoner som er mer ekstreme enn det har vært mulig å forutse. Hva da? Når beredskapsplanen ikke strekker til. Eller når det gis ordre eller instrukser som ikke reflekterer en generelt akseptert norm. Hva som er den aksepterte normen blir noen ganger ikke klart før historien skal skrives.

For at det enkelte menneske skal gjøre riktige handlingsvalg, må de ha tillit fra de styrende til å agere i henhold til de verdiene som er forankret i omgivelsene og reflektert i organisasjonen. Jeg beveger meg her i retning av nødrett og sivil ulydighet, og det skal ikke drøftes videre. Poenget her er at når uforutsette hendelser oppstår, er en god løsning avhengig av enkeltmennesker som handler i henhold til et forankret verdigrunnlag, selv om det skulle være i strid med reglementet. I Høyers (Høyer, upublisert) terminologi forutsettes det en tykk institusjonell forståelse for å ha det rette forholdet mellom tillit og kontroll, slik at de beste handlingsalternativ velges.

Finner vi noen slik erkjennelse av enkeltindividers betydning i de styringssignalene som er gitt? Nei på overordnet nivå er det ikke spor av en slik erkjennelse i styringsdokumentene. Men det er ikke overraskende. Det er et naturlig utslag av hierarkiet at staten styrer sine organisasjoner og samfunnsutviklingen for øvrig, mens organisasjonen styrer sine ansatte. Men staten gir noen føringer og setter noen rammer for hvordan informasjonsssikkerhetsarbeidet skal utføres i den enkelte organisasjon. Som vi har sett på tidligere opplever i hvert fall mange kommuner at det er krevende å etablere et informasjonssikkerhetssystem i henhold til de krav som settes. Noen tar til og med snarveier for å få på plass den dokumentasjonen som kreves. Det er ikke overraskende at hvis det oppfattes som ressurskrevende å oppfylle de instrumentelle kravene i lov og forskrift, vil ytterligere ressursbruk på opplæring av ansatte m.v. være vanskelig å prioritere. Det er rasjonelt å oppfylle de kravene som er underlagt et tilsyn, selv personvern for den enkelte ikke oppnås. Dette kan bli konsekvensen av en sterk instrumentell styring. Slik det er dokumentert i flere av de referansens som er oppgitt, ville det trolig vært rasjonelt å legge større vekt på opplæring og holdningsskapende arbeid internt i organisasjonen for å sikre brukere og ansatte et personvern. Ergo en mer institusjonell forståelse av organiseringen og styinginssignalene.

Det er satt krav om en del dokumentasjon som må være på plass i den enkelte organisasjon. Utfordringen for organisasjonen er å innfri disse kravene. Her vil det som tidligere nevnt være nødvendig med en tykk institusjonell forståelse (Høyer, upublisert) i gjennomføringen siden personvernutfordringene ofte er uoversiktlige. Det ligger i begrepet tykk institusjonalisme at valg av handling og oppgaveutførelse er forankret i verdier og normer og ikke bare i regler og rutiner.

Forutsetningen for at den institusjonelle tilnærmingen skal resultere i ønskede handlinger hos den enkelte, er at verdien personvern har et riktig fokus. Eller for å si det på en annen måte: erkjennelse av at personvern er noe enkeltindividet har krav på, og derfor representerer en verdi for enkeltindividene. En bevissthet om at organisasjonens omdømme er en annen verdi selv om noen av tiltakene eller virkemidlene er de samme.

Begge de statlige organisasjonenen A og B oppgir at forvaltning av et godt omdømme for organisasjonen er viktig. Når personvern som verdi konverteres til en omdømmeverdi, endres fokus. Dette øker risikoen for at personvernet ikke ivaretas på en god nok måte. Dette viser at selv om det å ivareta eget omdømme kan være en institusjonell tilnærming, sikrer ikke dette uten videre et godt resultat for personvern. Det kreves at normer og verdier er reflektert til rett

subjekt. For offentlige organisasjoner som i alminnelighet er til for borgerne, og ikke for seg selv, kan det bli feil at organisasjonen setter seg selv i fokus.

Verken de andre forskningsarbeidene jeg har referert til, eller den organisasjonsteorien jeg bygger på, problematiserer opplæring av ansatte utover at det er viktig. Min forståelse er at styring av organisasjoner og styring av medarbeidere må underlegges en ulik logikk. Et eksempel for å forklare mitt poeng: videregående skole styres etter indikatorer og måltall som blant annet refererer til fravær, gjennomsnittlig karakter og hvor mange som fullfører og hvor mange som slutter. (Utdanningsdirektoratet, 2014) Jeg skal ikke ha noen mening om dette er fornuftige styringsparametere. Poenget er at dersom disse indikatorene videreføres som krav til den enkelte lærer, vil virkningen bli en annen enn om det holdes på organisasjonsnivå. Det er trolig for mye å forvente at den enkelte lærer skal rapportere etterrettelig på disse indikatorene dersom også hans insats vurderes på samme grunnlag.

Det synes som det langt på vei er en slik videreføring av sentrale føringer som skjer på personvernområdet. De sentrale styringssignalene og kravene blir i liten grad oversatt ved operasjonaliseringen overfor den enkelte medarbeider. Det å ikke gjøre noe er også atferd. Det er ikke identifisert at organisasjoner benytter sin styringsrett for å strukturere informasjonssikkerhetsarbeidet utover de sentrale føringene.

Lovbestemte føringer forblir krav som organisasjonen er forpliktet til å oppfylle, og som «noen» ansatte må sørge for blir innfridd. Opplæring og kompetanseoppbygging er viktig, men hva og hvordan? Uansett er det slik at kunnskap ikke uten videre er atferd, og det må i alminnelighet tilføres ytterligere insentiver eller eller annet. Det er her verdiforankringen, eller den institusjonenne tilnærmingen kan fylle en funksjon, og bidra til en god måloppnåelse.

Øvrige krav til medarbeidere

Jeg skal nå se på hva som på annen måte kreves av den enkelte medarbeider for å oppfylle de sentrale kravene, og ved det sørge for at personvernet er en realitet. Jeg har tidligere brukt eksemplet med utarbeidese av risikoanalyser, og skal her bygge videre på det.

Utarbeidelse av risikoanalyser og avviksrapportering er avhengig av kompetanse, evne og vilje hos de medarbeiderene som skal utføre oppgaven. Tranvik (Tranvik, 02/12) peker på at utarbeidelse av slike dokumenter ofte skjer langt ned i organisasjonen, og langt fra rådmannen som er ansvarlig. Dette kan selvsagt ha betydning for dokumentenes interne status, men jeg tror ikke det er avgjørende for kvaliteten.

Særlig risikoanalyser er en krevende øvelse. Ved utarbeidelse av risikoanalyser vurderes sannsynlighet for og konsekvens av ulike mulige hendelser, som sammen skal tegne et bilde av risikoen. Dette er en subjektiv vurdering som selvsagt kan være ganske forskjellig fra menneske til menneske. Logikken er at bare det er et tilstrekkelig antall deltakere vil det skapes et nærmest objektivt bilde. Jeg skal diskutere hvordan den menneskelige hjernen vil fungere ved disse vurderingene. Diskusjonen bygger på Kahnemans bok «Tenke, fort og langsomt» (Kahneman, 2012).

Den grunnleggende utgangspunktet til Kahneman er at hjernen tenker på to ulike måter. Det er ikke begrepsbruken i denne boken, men for enkelhets skyld kaller jeg de to systemene «intuitiv» og «rasjonell». Det er tilstrekkelig for å illustrere mitt poeng her. Selv om vi liker å oppfatte oss selv som rasjonelt tenkende mennesker, vil begrenset kapasitet føre til at utgangspunktet som oftest er en intuitiv konklusjon. I tillegg hevder Kahneman at den rasjonelle delen av hjernen er lat. Den rasjonelle siden vil derfor bare kvalitetssikre standpunktet, og godkjenne eller forkaste det intuitive. Dette innebærer at en rasjonell tenkning bare gjøres når den intuitive tanken forkastes, eller vi er bevisst at «dette må vi tenke mer på». En slik bevissthet kan skapes ved kunnskap om at vi ikke uten videre tenker rasjonellt.

Utgangspunktet i en risikoanalyse er å identifisere mulig hendelser for deretter vurdere sannsynlighet og konsekvens. Vi kan langt på vei overskue det vi vet at vi ikke vet. Men det vi ikke vet at vi ikke vet, er vanskelig å forholde seg til. Dette betyr at vi må ta høyde for at vi ikke klarer å identifisere alle mulige hendelser, og følgelig også må ha med hendelser vi ikke evner å se i vurderingen.

Hvor sannsynlig er det at hendelsen vil oppstå. Sannsynlighet er kanskje det mest krevende å gjøre gode vurderinger av. Bare tenk på hva ulik fagbakgrunn eller tilnærming kan bety. En statistiker vil ha en ganske annen forståelse av sannsynlighet enn en logiker eller filosof. Vurdering av sannsynlighet vil nødvendigvis måtte være subjektiv. Den bedømmingen vi gjør vil ligne på den vi gjør for fysiske forhold som avstand og størrelse. Ved vurderingen av slike fysiske forhold har de fleste av oss erfart at vi ofte kan ta feil. Avstandsbedømmelse vil blant annet være påvirket av hvor tydelig eller klart vi ser et objekt. Konsekvensen av det er at vi lett undervurderer avstanden når det er klart, og overvurderer avstanden når sikten er dårlig. Hvis vi overfører dette til sannsynlighetsvurderingen i en risikoanalyse vil en intuitiv tanke lett føre til at de hendelsene som står klart frem for oss, også blir vurdert som mer sannsynlige.

De som er mer utydelig beskrevet vil kunne bli undervurdert og klassifisert som mindre sannsynlige uten at det nødvendigvis er riktig. Og hva med de mulige hendelsene vi ikke evner å se, hvordan skal vi vurdere sannsynligheten for slike? Det var få som forutså Berlinmurens fall, 22. juli hendelsene i Norge, eller finanskrisen. Mer om det uforutsigbare kan blant annet finnes i The Black Swan (Taleb, 2010). Det har ofte det til felles at de oppstår sjeldent, men konsekvensene er store. Slike kan vannskelig innkluderes i en risikomatrise, men bevissthet om slike muligheter, bør være til stede.

En annen fare for at vi vurderer sannsynligheten feil, er koblet til representativitet. Hvis en hendelse som likner på en annen som vi vet ofte kan oppstå, vil vi også intuitivt tenke at det er sannsynlig at også denne hendelsen vil oppstå med en høy grad av sannsynlighet. Representativitet eller frekvens er ikke det samme som sannsynlighet, men vi vil lett trekke den slutningen likevel.

Dette er bare et par eksempler som viser at uten en rasjonell reflektert tilnærming vil sannsynlighetsvureringen kunne vektes feil.

Hvilke konsekvenser en hendelse vil få vil kunne vurderes utfra ulike typer konsekvenser. Disse vil ikke nødvendigvis ha samme måleenhet. Hvordan skal en kunne rangere konsekvenser som:

- Tap av personvern for den enkelte
- Tap av godt omdømme for organisasjonen
- Økonomiske kostnader

Disse enkle eksemplene viser at hvilken tallverdi en vil sette på den enkelte konsekvens, vil avhenge av hvilket perspektiv en har. En økonomidirektør vil trolig rangerer økonomiske konsekvenser høyt, mens informasjonssjefen kanskje er mer bekymret for tap av omdømme.

I en risikovurdering defineres risikoen som et produkt av sannsynlighet og konsekvens. Så gjøres det en vurdering av hva som er akseptabel risiko. Dette kan f.eks. se slik ut i en tabell hvis en ser bare på en hendelse:

		Konsekvens			
Sannsynlighet		Ufarlig	Uheldig	Alvorlig	Kritisk
	Lite sannsynlig	1	2	3	4
	Moderat sannsynlig	2	4	6	8
	Sannsynlig	3	6	9	12
	Svært sannsynlig	4	8	12	16

Her er uakseptabel risiko vurdert i feltet nede til høyre hvor tallverdien er høyest. Hvor grensen for uakseptabel risiko går, er gjerne bestemt på forhånd. Hva er grunnlaget for hvor grensen settes? Også her vil dette bero på subjektive vurderinger. Mennesker har et svært ulikt forhold til risiko. Noen er risikovillige og noen har risikoaversjon. Ulik tilnærming til og forståelse for risiko kan gi utslag på opp mot 50% differanse i følge Kahneman (Kahneman, 2012) Dette kan i ytterste konsekvens gi store utslag på en vurdert risiko. Om en risiko er satt til 12 kan den i realiteten like gjerne være 6 som 18.

Når risikoen er matamatisk beregnet, er engentlig øvelsen ferdig. Men, det ligger i tankens natur at vi vurderer om svaret er rimelig. Denne etterrefleksjonen vil kunne føre til at det blir foretatt justeringer slik at svaret føles riktig. Det er en alminnelig observasjon, i følge Kahneman, at mennesker blir mer risikosøkene hvis alle alternativ er dårlige. Det kan bety at der mange mulige hendelser har en uaksptabel risiko, vil vi lett kunne fristes til å justere risikomatrisen slik at den blir mer spiselig. Det er også et poeng at i forhold til uakseptable risikoer må det settes inn tiltak. Dette kan generere krav til aktiviteter som må utføres, og det har man kanskje ikke verken tid eller lyst til. Dette kan også påvirke til at mulige hendelser flyttes over til klassen for akseptabel risiko.

Jeg har over diskutert noen eksempler på at de kravene som er gitt fra nasjonale myndigheter på personvernområdet, er krevende å gjennomføre på individuelt nivå. Det forutsetter bevissthet fra organisasjonens ledelse, og ikke minst kreves det tilstrekkelig kompetanse og kapasitet hos medarbeiderne. Slik jeg ser det er de instrumentelle kravene som er satt svært vannskelig å oppfylle med god kvalitet. Om de i seg selv vil kunne føre til et godt personvern, er heller ikke gitt. En særlig utfordring er at når styringen og rapporteringen ofte er knyttet til tallstørrelser, skaper det i seg selv en illusjon av sannhet. Jeg vet av egen erfaring at det jeg kaller “excel-arumentasjon”, har stor gjennomslagskraft. Kanskje større enn den noen ganger fortjener?

Det er etter dette grunnlag for å hevde at sikkerheten sitter mellom ørene. Dette gjelder også informasjonssikkerheten og således også personvernet. En slik erkjennelse må komme på plass både i reguleringen, og styringssignalene som gis både sentralt og i den enkelte organisasjon.

6. Konklusjoner

Jeg skal i dette kapittelet se på om de undersøkelsene, diskusjonene og drøftelsene som er foretatt har gitt noen svar på mine undringer.

Forskningsspørsmålet jeg reiste innledningsvis var: Hvorfor har vi ikke et godt personvern i offentlige organisasjoner? Dette hadde sitt utspring i en førforståelse av at personvernet er dårlig ivaretatt. Denne oppfatningen bygget på oppslag i media, egen erfaring fra offentlig virksomhet og den oppmerksomheten det får fra både Datatilsynet, KS og andre.

Det er avdekket at flere offentlige organisasjoner har betydelige utfordringer med informasjonssikkerheten. Både Riksrevisjonen (Riksrevisjonen, 2014) og Datatilsynet (Datatilsynet, 2014) har rapportert om det. Det kan ikke derfra konkluderes med at personvernet generelt er dårlig ivaretatt i offentlige organisasjoner, men at det er et ikke ubetydelig problem synes klart.

Det kan derfor konkluderes med at: Forskningsspørsmålet er både relevant og interessant å se nærmere på.

Jeg reiste etter dette **problemstillingen** om årsaken til dårlig personvern i offentlige organisasjoner kan forklares med hvordan de styres. Styring ble drøftet i forhold til flere perspektiver. Fra statens overordnede styring gjennom lovregulering og andre føringer, via styring i den enkelte organisasjon, og til styring av medarbeiderene. Problemstillingen er diskutert både i forhold til utvalgt empiri, litteratur og teori.

Både Datilsynets undersøkelse (Datatilsynet, 2014) og Tranviks undersøkelse (Tranvik, 02/12) viser til at forankringen og innvolveringen fra ledelsen ofte er svak eller mangler helt. Konsekvensen av det er at når det er en vilje til å etablere informasjonssikkerhet, er det en eller flere medarbeidere som gis ansvaret for dette. Det operasjonaliseres ved at den sentrale styringen "påføres" medarbeiderene direkte. De kravene som er satt der oppleves som vanskelige å forstå, og arbeidskrevende å etablere.

Dette viser at den overodnede statlige styringen har betydning for oppgaveutførelsen på organisasjonsnivå. Og styringen der har betydning på minst to måter: hva som faktisk gjøres i organisasjonen, og hvordan det gjøres. Det er vist til at det som gjøres er på bakgrunn av den statlige instrumentelle styringen som gjennom lov og forskrift pålegger organisasjonene

nærmere angitte oppgaver, og krav om å etablere et systemregime. Om dette i seg selv reduserer styringsviljen i organisasjonenes ledelse er ikke identifisert, og står tilbake som en mulig antakelse.

Jeg har i min drøftelse diskutert om styringssignalene er egnet til å etablere målet "godt personvern". Svaret jeg gir er at styringssignalene kan være feil, og de er i hvert fall ikke tilstrekkelig. På organissjonsnivå er det få spor av ytterligere styring. Noen synes å ha en oppfatning av at delegering og budsjettering er tilstekkelig styring alene.

Det er ikke tvilsomt at styringen er en medvirkende årsak til dårlig personvern i offentlige organisasjoner. Andre mulige årsaker som er drøftet, er knyttet til medarbeidernes oppgaveutførelse. Alternative medvirkende eller utløsende årsaker er ikke undersøkt, og det kan derfor ikke utelukkes at det også er andre årsaker som påvirker til dårlig personvern.

Hypotesen jeg reiste var at en større grad av institusjonell tilnærming gir bedre personvern. Dette viste seg vannskelig å undersøke videre på bakgrun av de empiriske undersøkelsene. Årsaken til det er at det er få eksempler på institusjonell forståelse av organisasjoene. De forskingsarbeidene som er drøftet hadde ikke undersøkt denne hypotesen, eller for så vidt ikke problematisert denne tilnærmingen overhodet. Ingen av mine intervjuerobjekter har en slik tilnærming til den enkeltes rett til personvern. De har likevel en institusjonell tilnærming, men da i forhold til verdien å ivareta eget omdømme. Dette fokuset synes å bidra til å ivareta et hemmelighold, og på den måten etablere et personvern. Jeg har i min drøftense lagt til grunn at dette ikke er tilfredstillende og betryggende for personvernet. Min konklusjon er at en institusjonell tilnærming også må være forankret i "riktige" verdier for at hensikten skal oppnås.

De nasjonale styringssignalene reflekterer ikke noen bevissthet om institusjonell tilnærming.

Mye organisasjonereori, og særlig Høyer (Høyer, upublisert), konkluderer med at tykk institusjonell forståelse er ønskelig for å løse oppgaver som har stort utfallsrom eller med diffuse mål. Instrumentell tilnærming, det som Høyer kaller tynn institusjonell forståelse, er eventuelt egnet for mer "samlebåndpreget" oppgaveutførelse.

Konklusjonene fra teorien er ikke reflektert i de nasjonale styringssignalene.

Organisasjonsnivået, enten det er kommunalt eller statlig, er ikke preget av noen selvstendig forankring i institusjonell organisasjonsteori. Det synes som statlig styring langt på vei

kopieres over til den enkelte organisasjon, og hos disse er som nevnt ikke noen institusjonell tilnærming synlig på det området som er undersøkt.

Konklusjonen er derfor at hypotesen ikke kan verifiseres.

Det er i seg selv et interessant funn at det som er reist som en fornuftig tilnærming av teoretikere i litteraturen, finnes det ikke spor av verken i styringssignaler eller praksis. Et nærliggende nytt forskningsspørsmål er om de siste ti-års fokus på New Public Management har gjort de styrende blinde for andre organisasjonsteoretiske tilnærminger.

Jeg vil avslutte mer å sitere Ninni Sandvik (Ph.D.) fra et intervju i tidskriftet "Første steg":

«Jeg fikk gjøre hva jeg ville fordi ingen andre hadde tatt seg bryet med å sette seg inn i sakene. Når storebror ikke ser deg, kan lillesøster gjøre som hun vil i skyggen – det er slik jeg tenker.» (Solli, 2014 nr 3)

Jeg tar dette sitatet ut av sin sammenheng, men på området personvern kan realiteten bak utsagnet være både positivt og negativt.

Det vil ha en positiv virkning dersom man tenker at så lenge noe statlig tilsyn ikke kommer, kan jeg etablere det personvernet enhver har krav på. Underforstått at en ikke trenger bruke ressurser på utjenlig regelverk.

Det vil ha en negativ konsekvens hvis organisasjonen tenker at så lenge vi ikke får noe tilsyn som pålegger oss en aktivitet, bruker vi resursene på viktig tjenesteproduksjon. Underforstått en trenger ikke en gang å skape noen etterlevelsesillusjon før de styrende tvinger oss. Da er verdien personvern helt fraværende og forvaltning av eget omdømme er det eneste som er tilbake.

Jeg slutter meg til Brunsons (Brunson, 2006) refleksjon om at det er viktig å holde fast ved

håpet.

7. Etter-refleksjoner

Dette kapittelet inneholder noen refleksjoner knyttet til de valgene som er gjort i forskningsarbeidet og prosessen som sådan. Det starter med et metablikk på forskningsprosessen og rollen som forsker, herunder prosessen med selve skrivearbeidet. Videre er det knyttet noen kommentarer til den etiske dimensjonen ved valgene som er gjort. Til slutt en vudering av oppgavens validitet og mulig overføringsverdi.

7.1 Egen forskerrolle og forskningsprosess

Jeg har hele tiden forsøkt å være besvisst at min bakgrunn som jurist og at min yrkesmessige tilknytning til temaet, ikke i for stor grad skal prege forskerrollen i dette arbeidet. I hvilken grad jeg har lykkes med det, må andre vudere.

Rollen som forsker er krevende, og særlig det å holde orden på alle "løse tråder" tidlig i prosjektet opplevdes som vanskelig. Etterhvert ble mange av trådene festet på riktig sted, og de andre har blåst avsted når jeg slapp taket.

Selve forskningsprosessen er gjennomført etter en plan. Etterhvert som arbeidet skred frem ble det avdekket ny kunnskap som påvirket valgene. Valg av empirisk grunnlag ble endret slik det er redegjort for, og valget har gitt så mye informasjon som det var grunn for å håpe på.

Det er med ydmykhet jeg har møtt de jeg har bedt om bidrag i mitt forskningsarbeid. De har møtt meg og svart på mine spørsmål med oppriktig interesse. Som en av informatene sa; personvern et tema for spesielt interesserte. Det å møte andre som er levende opptatt av personvernet og hvordan vi skal ta vare på det, er inspirerende i seg selv.

7.2 Skrivearbeidet

Selve skriveprosessen er mye mer enn det å skrive selve masteroppgaven. Fra de refleksjonsnotatene som ble skrevet i forbindelse med forelesninger og kollokvie-arbeid, til den ferdige masteroppgeven er det flere steg. Både jobben med formulering av problemstilling og hypotese samt transkribering av intervjuer, ser jeg på som en del av skriveprosessen. Alle disse formene for skriving har gitt meg verdifulle refleksjoner underveis, og er av betydning for den ferdige masteroppgaven. Hver gjennomlesning av avsnitt eller hele teksten, gir nye

refleksjoner og nye impulser for skrivingen. På den måten tar skriveprosessen aldri slutt. På samme måte som et hvert forskningsarbeide sjelden setter punktum for noe, men et kolon for videre bearbeiding. Noen har bestemt en frist, og derfor er denne masteroppgaven slik den er ved fristen.

7.3 Etiske vurderinger

Det er ikke personlige forhold, eller andre typer hemmeligheter i seg selv som er behandlet, og det er derfor ikke dilemmaer knyttet til bruk av opplysninger. De som har latt seg intervjue har gitt sitt samtykke på bakgrunn av min presentasjon av prosjektet. De har kunnet trekke sitt samtykke når som helst, og jeg setter peis på at de ikke har benyttet seg av denne retten. Likevel har de gitt meg informasjon i tillit til at jeg behandler den etterrettelig og med respekt, men de har ingen innflytelse på hvordan jeg tolker og bruker opplysninger de har gitt. Jeg har gjort mitt beste for ikke å misbruke den tilliten jeg er vist.

7.4 Validitet

Validitet betyr rett og slett gyldighet. Jeg skal her vurdere validiteten til arbeidets begrepsbruk og konklusjoner.

Begrepsbruken "instrumentell" og institusjonell" er forklart og har en forankring i teori. Teorien er noe sprikende både over tid og mellom ulike forfattere i forhold til inneholdet i disse begrepene. Noen benytter også andre begrep for noe tilsvarende. Det kan være grunn til å kritisere at min begrepsbruk er en popularisering, og det er nok et stykke på vei riktig. Den begrepsavklaringen som er foretatt mener jeg likevel gjør begrepsbruken valid.

Konklusjonen om at måten det styres på, og hvilke styringssignaler som gis, er et viktig årsaksfaktor for om mål oppnås, er ikke oppsiktvekkende. Dette vil være åpenbart for de fleste. Her ligger det en utfordring i seg selv: det åpenbare eller det inneforståtte trenger også å underlegges en kritisk vurdering. Jeg har diskutert styringen og kommet med eksempler som styrker konklusjonen. Konklusjonen om at styringen er viktig for måloppnåelsen er valid.

Hypotesen om at en større grad av institusjonell tilnærming gir bedre personvern, kan ikke verifiseres. Årsaken ligger i at jeg ikke har funnet noen organisasjon som har en slik tilnærming til personvern. Innenfor rammen av denne oppgaven er denne slutningen valid.

Det er interessant at tanker som er presentert av teoretikere i hvert fall de siste 50 år ikke er reflektert i praksis. Jeg har selvsagt ikke full oversikt over praksisfeltet, slik at dette er ikke et valid utsagn. Men interessant er det.

Et siste spørsmål er om konklusjonene og diskusjonene har noen overførbarhet. Det er det vannskelig å ha noen sikker oppfatning om, men det kan være gunnlag for ytterligere undersøkelser. En nærliggende antakelse er at andre mål som er lite målbare også bør underlegges en styring som er preget av mer institusjonell forståelse. Det er imidlertid ikke grunnlag for å hevde at en slik oppfatning er en valid. Det må undersøkes flere likeartede tilfeller før det eventuelt kan være grunnlag for en generalisering.

Litteraturliste

Alvesson, M., & Deetz, S. (1996). *Critical theory and postmodernism approches to organizational studies.* London: Sage.

Aubert, V. (1982). *Rettssosiologi.* Oslo: Universitetsforlaget.

Brunson, N. (2006). *Mechanisms of Hope Maintaining the Deam of the Rational Organizatoin.* Universitetsforlaget.

Busch, T., Vanebo, J. O., & Dehlin, E. (2010). *Organisasjon og organisering.* Oslo: Universitetsforlaget.

Cooper, R., & Burell, G. (1988). *Modernism, post modernism and organizational analysis: An introduction, Organizatio studies.*

Datatilsynet. (2014, 10 23). Hentet fra http://datatilsynet.no/Personvernombud/

Datatilsynet. (2014, 11 09). *Datatilsynet.* Hentet fra datatilsynet.no: http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Analyser-utredninger/Kommuneundersokelsen-2010-2011-/

Datatilsynet. (2014, 10 11). *Datatilsynet*. Hentet fra www.datatilsynet.no: http://datatilsynet.no/Om-Datatilsynet/

Datatilsynet. (2014, 10 15). *datatilsynet.no*. Hentet fra http://www.datatilsynet.no/verktoy-skjema/Ordbok-A-til-A/#K

Datatilsynet. (2014, 09 10). *Hva er personvern.* Hentet fra Datatilsynet.no: http://www.datatilsynet.no/personvern/Hva-er-personvern/

DIFI. (2014, 10 08). *www.difi.no*. Hentet fra http://www.difi.no/digital-forvaltning/informasjonssikkerhet

DiMaggio, P. J., & Powell, W. W. (1991). *The iron cage revisted: Institusjonal isomorphism and collective rationality in organizational fields.* Chicago: The University of Chicage Press.

Eriksson-Zetterquist, U., Kalling, T., & Alexander, S. (2012). *Organisation och organisering.* Malmö: Liber AB.

Fasting, M. (2014, februar 3). *Civita.* Hentet fra www.civita.no: http://www.civita.no/2014/02/03/foler-du-deg-overvaket

Gjørv, A. B. (2012, 11 13). *regjeringen.no.* Hentet fra http://www.regjeringen.no/pages/37994796/PDFS/NOU201220120014000DDDPDFS.pdf

Høyer, H. C. (upublisert). *(under forberedelse): Tillit og kontroll - som ild og vann eller som sukker og kanel, antologi om styring, kontroll og tillit under utgivelse.*

Idsø, J. &.-a.-t. (u.d.).

Kahneman, D. (2012). *Tenke, fort og langsomt.* Pax forlag.

Kommunal og moderniseringsdepartementet. (2014, 10 20). *Regjeringen.* Hentet fra http://www.regjeringen.no/nb/dep/kmd/dok/tildelingsbrev-tilskuddsbrev.html?id=522666

lovdata. (u.d.). *Lovdata.* Hentet fra lovdata.no: http://lovdata.no/lov/1999-05-21-30/emkn/a8

Mach, J. G. (1995, 2. utgave 2008). *Fornuft og forandring.* Frederiksberg: Forlaget Samfunsliteratur.

Mach, J. G. (2008). *Fornuft og forandring.* Forlaget Sammfundslitteratur.

Najonal sikkerhetsmyndighet. (2013). *uninett.no.* Hentet fra Presentasjon på sikkerhetsforum 2013: https://www.uninett.no/webfm_send/739

Norsk senter for informasjonssikring. (2014, 10 11). *www.norsis.no*. Hentet fra Norsis: https://norsis.no/om-norsis/

NOU 2012:14. (2014, 10 19). *Regjeringen.* Hentet fra http://www.regjeringen.no/pages/37994796/PDFS/NOU201220120014000DDDPDFS.pdf

PwC. (2014, 09 11). *Kommunenes sentralforbund.* Hentet fra ks.no: http://www.ks.no/PageFiles/49909/Sluttrapport%20forsvarlig%20behandling%20av%20dokumentasjon_TS.pdf

Reddick, C. G. (2009). Management support and information security: an empirical sudy of Texas state agencies i USA. ss. 361 - 377.

Regjeringen. (2014, 10 18). *Kommunal og moderniseringsdepartementet.* Hentet fra Regjeringen.no: http://www.regjeringen.no/nb/dep/kmd/dok/regpubl/stmeld/2008-2009/stmeld-nr-19-2008-2009-.html?id=552811

regjeringen. (2014, 09 10). *regjeringen.no.* Hentet fra kommunal og moderniseringsdepartementet: http://www.regjeringen.no/nb/dep/kmd/tema/personvern/hva-er-personvern.html?id=448290

Regjeringen. (2014, 10 18). *Regjeringen.no.* Hentet fra http://www.regjeringen.no/pages/38164416/PDFS/STM201220130011000DDDPDFS.pdf

Riksrevisjonen. (2014, 10 16). Hentet fra Riksrevisjonen.no: https://www.riksrevisjonen.no/presserom/Pressemeldinger/Sider/Dokument1for2013.aspx

Selznick, P. (1957). *Leadership in administration.* London: University of California Press.

Senter for statlig økonomistyring. (2014, 10 20). *www.dfo.no.* Hentet fra http://www.dfo.no/Documents/FOA/publikasjoner/veiledere/Maal_og_resultatstyring_i_staten.pdf

Solli, A. (2014 nr 3). Trives best i opposisjon. *Første steg tidskrift for barnehagelærere*, ss. 28 - 31.

Svendsen, L. F. (u.d.). Svendsen, Lars Fredrik Händler. (2011, 7. desember). Intensjonalitet. I Store norske leksikon. Hentet 24. september 2014 fra https://snl.no/intensjonalitet.

Taleb, N. N. (2010). *The Black Swan: The Impact of the Highly Improbable Fragility.* . Random House LLC.

Tranvik, T. (02/12). Kommunal regeletterlevelse – Illusjoner og realiteter på personvernområdet. *Tidsskrift for samfunnsforskning*, 131 - 156.

Utdanningsdirektoratet. (2014, 10 24). *Skoleporten*. Hentet fra https://skoleporten.udir.no/oversikt/nasjonalvgo.aspx?enhetsid=00&skoletypemenuid=1&visHele=true

Øverenget, E. (2013, 10 25). Etikk og profesjon - ikke snill, men klok. Lillestrøm, Norge.

Norsk sammendrag

Mål

Denne oppgaven tar for seg personvern i offentlige organisasjoner. Søkelyset er rettet mot hvor godt eller dårlig personvernet er ivaretatt, og hva som er mulige forklaringer på det. Det er klarlagt at mange offentlige organisasjoner ikke er gode nok til å etablere et godt personvern. Det kommer til uttrykk ved at de ofte ikke har etablert de systempliktene som er fastsatt i personopplysningsloven med forskrift. Og om de har fått dette på plass, er det ikke uten videre gitt at det blir brukt, eller at denne dokumentasjonen gir et sant bilde av hva som faktisk blir gjort i organisasjonen.

Hvorfor er det slik? Forklaringen kan være at de nasjonale stryringssignalene er feil, og/eller at organisjonenes implementering av disse ikke fungerer.

I min studie er både perspektivet om ledelse og styring, og perspektivet institusjonell forståelse av organisasjonen, pekt på som forklaringer på manglende personvern.

Metode

Det er gjort undersøkelser både i Datatilsynets publikasjoner (f.eks. kommuneundesøkelsen (Datatilsynet, 2014)) og hos Riksrevisjonen (Riksrevisjonen, 2014) for å klarlegge dagens situasjon for personvernet i offentlige organisasjoner. Også andre referanser er konsultert for å få et bredere grunnlag for status.

Det er etter det gjort intervjuer både med Datatilsynet og med to store statlige organisasjoner. Opplysningene herfra er deretter drøftet opp mot målet for oppgaven. Det er også drøftet forholdsmessig mye teori fra litteraturen siden de empiriske undersøkelsene ga få relevante funn for mitt forskningsperspektiv.

Resultater

Diskusjonen rundt de sentrale styringssignalene viste at den retten hver enkelt har til personvern, er oversatt til en plikt for organisasjonene om å etablere informasjonssikkerhet. Målet er dermed formulert med feil subjekt i personopplysningsloven. Fokuset er flyttet fra en rett for individet til en plikt for organisasjonen.

Informasjonssikkerheten er beskrevet som et instrumentelt krav om å etablere et system med rutiner og prosedyrer, og disse skal dokumenteres. Empirien viser at dette ikke alltid fører til

et godt personvern. I beste fall reflekteres det over at brudd på plikten til hemmelighold kan utfordre omdømmet, og organisasjonen blir fokusert på å verne det gode omdømmet.

Det konkluderes med at både feil fokus i styringssignalene, og delvis ureflektert institusjonell forståelse er mulige forklaringer på manglende ivaretakelse av personvernet i offentlige organisasjoner.

Engelsk sammendrag (abstract)

Goals

This paper discusses the right to privacy as implemented by public organizations. Attention is directed at how well or how poorly the right to privacy is being safeguarded, and what are the possible reasons. It appears that many public organizations fall short of establishing a good policy in this field. This can be seen in the fact that they frequently fail to implement the system obligations under the Personal Data Act and Regulations. Even where this is in place, it does not automatically follow that it is being used, or that this documentation gives a correct picture of the actual practice within the organization.

Why is this so? The explanation may be that the national tow ring signals are incorrect and/or that the organization's attempts at implementing them do not work in practice. In my paper I examine leadership and management as well as the institutional understanding of the organization as possible explanations for the shortcomings referred to above.

Method

Surveys have been carried out both by the Norwegian Data Protection Authority (2014) and the Office of the Auditor General (2014) to clarify the current situation regarding the way in which the right to privacy is being implemented in practice by public organizations. Additional sources have been consulted in order to gain a more comprehensive basis for evaluating the current situation in this field. Subsequently, interviews have been conducted with the Data Protection Authority and two major government organizations. Information gleaned from these interviews has been used in my analysis. In addition I have consulted relevant literature extensively, as the empirical information produced by my research appeared to have limited bearing on my topic of study.

Findings

Debate focusing on the central control signals indicates that the individual's right to privacy has been translated into an obligation for the organizations to provide information security. The right of the individual is no longer the main subject as laid down in the Personal Data Act. Instead, the focus has been transferred from the right of the individual to the organization and its obligation to provide information security.

Information security is being described as an institutional obligation to establish a system of practices and procedures, all of which has to be documented. However, my empirical data

appear to indicate that this does not always lead to good policy. A breach of the duty of confidentiality may be seen as damaging to the organization's reputation, leading that organization to shifting its focus to protecting its reputation.

My findings appear to show that a wrong focus in the central control signals along with a partly unconsidered organizational understanding, may explain shortcomings in the protection of the right to privacy in public organizations.