

Forprosjektrapport

fra arbeidsgruppen
Regelverk og informasjonssikkerhet

til

Koordineringsutvalget for
informasjonssikkerhet
(KIS)

Oslo, 7. juni 2005

Innholdsfortegnelse

Sammendrag	4
1 Bakgrunn og mandat	6
1.1 Mål og mandat for forprosjektet	6
2 Arbeidsgruppens sammensetning og arbeidsmetoder	7
2.1 Beskrivelse av arbeidsmåte og metode.....	8
2.1.1 Kunnskapsnettverk	8
2.2.2 Dokumentstudier	8
3 Oversikt over regelverk med betydning for informasjonssikkerhet ..	10
3.1 Kartlegging.....	10
3.2 Om bruk av standarder	11
3.3 Om gjennomføring av internasjonale regler – forpliktelser og føringer.....	11
3.4 Regler uten egen tilsynsmyndighet.....	12
4 Noen erfaringer og mulige problemområder.....	12
4.1 Regelforvaltere	12
4.1.1 Moderniseringsdepartementet	12
4.1.2 Justisdepartementet	14
4.1.3 Samferdselsdepartementet.....	14
4.1.4 Forsvarsdepartementet	15
4.2 Tilsynsmyndigheter.....	16
4.2.1 Datatilsynet.....	17
4.2.2 Post- og teletilsynet	18
4.2.3 Kredittilsynet.....	20
4.2.4 Nasjonal sikkerhetsmyndighet (NSM).....	21
4.2.5 Norges vassdrags- og energidirektorat (NVE).....	23
4.3 Noen brukersynspunkter.....	24
4.4 Problembeskrivelse – analyse og vurderinger.....	25
4.4.1 Innledning.....	25
4.4.2 Analysemetode	25
4.4.3 Tidligere studier som omhandler regelverk om informasjonssikkerhet (offentlige utredninger og evalueringer).....	26
4.4.4 Analyse og vurdering av de rettslige reguleringene av informasjonssikkerhet	26
Økonomiske tiltak.....	31
4.4.5 Om veiledninger til reglene og bruken av dem.....	32
4.4.6 Manglende empiriske studier av rettsreglenes effekter.....	32
5 Anbefalinger	32
5.1 Notater om å ivareta informasjonssikkerhet ved hjelp av regelverk.	33

5.1.1	Introduksjon	33
5.1.2	Allment om regelverk vedrørende informasjonssikkerhet	34
5.1.3	Helhetlig blikk på regelverksarbeid	37
5.1.4	Motsatte perspektiver på regelstyring av informasjonssikkerhet 38	
5.1.5	Kommunikasjon av sikkerhetsregelverk	40
5.1.6	Samordning av sikkerhetsregelverk	44
5.1.7	Bruk av verktøy i tilknytning til utarbeiding, anvendelse og evaluering av sikkerhetsregelverk	48
5.1.8	Organisering av rettsanvendelse.....	52
5.1.9	Avsluttende bemerkninger	53
5.2	<i>Empiri og samordning</i>	53
5.2.1	Noen hovedfunn, som bakgrunn for forslag.....	53
5.2.2	Behovet for et bedre og empirisk basert beslutningsgrunnlag for videreutvikling av regelverkene om informasjonssikkerhet	54
5.2.3	Behovet for å se nærmere på hvordan regler om informasjonssikkerhet samordnes og koordineres.	56
5.3	<i>Kort gjennomgang av anbefalinger om tiltak</i>	56
5.3.1	Det settes i gang et kontinuerlig, systematisk og helhetlig arbeid – stikkord: ”regelverkssyklus og verktøy”	57
5.3.2	Samarbeid for regelverks- og tilsynsarbeidet.....	58
5.3.3	Bedre pedagogiske tiltak	60
5.3.4	Vurdere effekter av regelverket, empiri, evalueringer - etterkontroll	61
	Begrunnelse:.....	62
5.3.5	Andre tiltaksforslag	63
	Vedlegg	65
	Litteraturliste	65

Sammendrag

Arbeidsgruppen Regelverk og informasjonssikkerhet ble nedsatt av Koordineringsutvalget for informasjonssikkerhet (KIS). Bakgrunnen for prosjektet er Regjeringens strategi for informasjonssikkerhet for perioden 2003 - 2006. Gruppens mandat var å få frem en oversikt over regelverket, peke på mulige problemområder og ut fra dette komme med anbefalinger.

Arbeidsgruppens anbefalinger skal i første rekke være et startgrunnlag for KIS i deres videre arbeid med å følge opp og bidra til implementeringen av den nasjonale strategien i forhold til regelverk og informasjonssikkerhet.

I kapittel 2 vises det til arbeidsgruppens sammensetning og arbeid.

Arbeidsgruppen har bestått av deltakere fra Post- og teletilsynet, Kredittilsynet, Datatilsynet, Forsvarsdepartementet, Nasjonal sikkerhetsmyndighet, Universitetet i Oslo (AFIN) og Statskonsult, som har ledet arbeidet, på oppdrag fra KIS/Moderniseringsdepartementet. Det gis også en kort oversikt over fire verdifulle kilder til informasjon (kapittel 2.2.2); en ny bok¹ med gjennomgang av de viktigste regelverksområdene for informasjonssikkerhet, en forskningsrapport fra forsker/stipendiat Are Vegard Haug (AFIN), en veiledning med oversikt over lover og regler med betydning for informasjonssikkerhet laget og utgitt av IT-sikkerhetsForum (ISF), og til slutt en utredning om risikovurdering og sikkerhetsstyring – metoder og verktøy, skrevet av Johs. Hansen Hammer, på oppdrag for Nærings- og handelsdepartementet, med et sideblikk til de mest sentrale regelverkene.

I kapittel 3 er det gjort rede for oversikt over regelverk med betydning for informasjonssikkerhet. Dette er gjort kort, fordi det vises til de mer omfattende originalkildene til kunnskap om dette; i hovedsak Haugs og Schartums arbeider, samt den nevnte boken, med Jansen og Schartum fra AFIN som redaktører.

I kapittel 4 gis det noen erfaringer og mulige problemområder, ut fra arbeidsgruppens syn. Oversikt over ansvarsområdene til og erfaringene fra Moderniseringsdepartementet, Samferdselsdepartementet, Forsvarsdepartementet, Datatilsynet, Post- og teletilsynet, Kredittilsynet og Nasjonal sikkerhetsmyndighet gis, samt et innspill vi mottok fra Norges vassdrags- og energivesen. Det gis også noen relativt få innspill fra brukersiden, nærmest som smaksprøver. En fylldig problembeskrivelse og analyse er gitt i 4.4.4, skrevet av Haug.

Arbeidsgruppen har ikke selv gått gjennom alle regelverkene som det er funnet frem til. Det har derimot Haug, i egenskap av forsker, som også har deltatt i gruppen. Han har uavhengig av arbeidsgruppens arbeid gjennomført ett års forskningsprosjekt i hovedsak forut for arbeidsgruppens arbeid, som vi har vært så heldige å få nytte godt av. En del av Haugs forskning er tatt med i denne rapporten (særlig i kapittel 4.4 og 5.2, samt de omfattende vedleggene 1 og 4). Vedleggene til rapporten finnes i et separat vedleggsnotat.

¹ *Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT*, Arild Jansen og Dag Wiese Schartum (red), Fagbokforlaget, 2005.

I kapittel 5 kommer arbeidsgruppens anbefalinger. Det vil si: i 5.1 gir dr. juris Dag Wiese Schartum sin gjennomgang og "fritenkning med nye øyne", og konkluderer med et forslag som har stikkordet "*regelverkssyklus og verktøy*". Han gir her en skisse til hvordan det kan arbeides med å forbedre regelverk for informasjonssikkerhet i Norge, og konkluderer med et forslag som har som mål at vi til sammen får et mer helhetlig og systematisk grep enn i dag, og på mer kontinuerlig basis. Schartums forslag er det mest prinsipielt omfattende og innholdsrike vi har å by på. Videre følger Haug godt opp i 5.2 ved å gå gjennom noen av sine hovedfunn fra kartlegging og gjennomgang, og understreker sterkt at vi må få bedre empirisk materiale å bygge på enn i dag. Han viser også en mulig modell for å bidra til dette. På denne bakgrunnen, og på bakgrunn av arbeidsgruppens i all beskjedenhet ikke ubetydelig samlede erfaring og kunnskaper, gis det i kapittel 5.3 en rekke anbefalinger til tiltak for å forbedre situasjonen på området regelverk og informasjonssikkerhet i Norge. I kapittel 5.3 har vi ikke lange, resonerende tekster, men har forsøkt å fremstille anbefalingene om tiltak i en komprimert, oversiktlig og lesevennlig form. De gir innspill til noen hovedretninger, men låser ikke fast til (for) mange detaljer. Det er et håp at KIS kan få en rask oversikt over forslagene ved å lese 5.3, fortrinnsvis ved først å ha lest 5.1 og 5.2, som gir en nødvendig bakgrunn.

Anbefalingene har som mål å bidra til å styrke både samfunnets interesse i oppnå bedre og mer effektiv styring via eksisterende og kommende regelverk, og brukernes interesse i at de juridiske normene blir enklere å leve med, på en kostnadseffektiv måte. Anbefalingene skal dermed selvfølgelig også støtte regelverkens målsetting om bedre faktisk informasjonssikkerhet i samfunnet, enten synsvinkelen er ut fra behovene i finansnæringen, på personvernområdet, i næringslivet eller i offentlig forvaltning.

Arbeidsgruppens anbefaling i kapittel 5.3 er fordelt på noen hovedoverskrifter: *Regelverkssyklus og verktøy*; forslag om å sette i gang konkrete arbeider så fort som mulig, med fokus på kontinuerlig, systematisk og helhetlig arbeid knyttet til regelverkens "livssyklus" – forarbeid (og vedtak), anvendelse, evaluering, der hvert trinn eller fase blir en forberedelse for det neste. *Samarbeid for regelverks- og tilsynsarbeidet*; forslag om å etablere en møteplass for mange aktiviteter av tverrgående karakter, blant annet felles opptreden/tilsyn, der dette passer. *Bedre pedagogiske tiltak*; forslag om å sette i gang mer systematiske og fremtidsrettede tiltak for å bidra til at regelverkene blir bedre formidlet, lettere å forstå, og lettere å etterleve. Blant annet forslag om bedre utnyttelse av internett til formidling av informasjon, og nettbasert læring. *Effekter av regelverk*; det spørres om vi faktisk har grunnlag for å vite om og hvordan regelverkene virker, som grunnlag for anvendelse/etterlevelse og fornyelse av reglene. Siden funnet fra kartleggingen er at vi knapt har empiri på området, foreslås det tiltak for bøte på dette, bl.a. konkrete studier, eksempelprosjekter og systematiske evalueringer (som peker tilbake på det første forslaget – stikkord regelverkssyklus og verktøy, også for bedre evalueringer). Til slutt er det samlet anbefalinger under "sekkeposten" *andre tiltaksforslag*; bl.a. forslag om i langt større grad enn i dag å vurdere felles underlag for flere regelverk ved bruk av standarder, lage sjekklister for internkontroll og informasjonssikkerhet, forslag om å lage et krav om erklæring i årsmeldingen fra ledelsen om samsvar mellom

liv og lære ut fra regelverkens krav om informasjonssikkerhet (gjærne stadfestet av uavhengig tredjepart), osv.

I kortform kan en si at arbeidsgruppen anbefalinger handler om dette:

- **Hvordan eksisterende og kommende regler om informasjonssikkerhet kan samordnes og koordineres**
- **Bedre muligheter for å rydde og forenkle begreper, struktur mv. i regelverket**
- **Bedre samordning av tilsynsarbeidet**
- **Måle effekter av regelverket, evaluering og etterkontroll**
- **Fremskaffe empirisk materiale**
- **Utvikle bedre tiltak som gjelder informasjon til brukerne**
- **Utvikle tiltak for kompetanseoppbygging for både myndigheter og brukere**
- **Ta i bruk elektroniske hjelpemidler på en mer avansert måte i alle deler av arbeidene som er nevnt over.**

1 Bakgrunn og mandat

Regjeringen vedtok i juni 2003 en *Nasjonal strategi for informasjonssikkerhet*, med undertittel *Utfordringer, prioriteringer og tiltak*. Dette var på felles initiativ fra Nærings- og handelsdepartementet, Justisdepartementet og Forsvarsdepartementet, med et tidsperspektiv på to – tre år.

Som et ledd i gjennomføringen av strategien er Koordineringsutvalget for informasjonssikkerhet (KIS) etablert. Deltakere er sentrale departementer og direktorater. KIS har deretter satt i gang en arbeidsgruppe for regelverk og informasjonssikkerhet, som innenfor en kort tidsramme legger frem denne rapporten. Hensikten er at KIS skal få et bedre startgrunnlag for sitt videre arbeid med å følge opp og implementere den nasjonale strategien – i denne sammenheng sett i forhold til regelverk og informasjonssikkerhet.

1.1 Mål og mandat for forprosjektet

Utgangspunktet for arbeidsgruppens arbeid står beskrevet i *Nasjonal strategi for informasjonssikkerhet tiltak II – Regelverk for IT-sikkerhet*:

- **Regelverksgjennomgang og samordnet håndheving** – Det bør settes i gang et arbeid i forhold til regelverk for informasjonssikkerhet, for å få de eksisterende reglene i bedre praktisk bruk, og gi bedre grunnlag for fornyelse og forenkling av de, inklusive spørsmålet om samordnet/ enklere håndheving. Arbeidet skal omfatte å lage en oversikt over reglene for informasjonssikkerhet, lage praktiske veiledninger, samt kurs og opplæring.
- **Utvikling av regelverk som berører IT-sikkerhet** – Den enkelte regelverksforvalter bør systematisk innhente opplysninger om hvordan regelverkene faktisk virker i praksis, og periodevis vurdere behovet for endringer i regelverket. Det skal arbeides for at regelverk som berører IT-sikkerhet utvikles på en mest mulig koordinert måte, at det gis klare og konsise regler, og at det gjøres klare avgrensninger mot andre

regelverk, slik at det ikke oppstår tvil om tolkningen eller om hvilke regler som gjelder i et gitt tilfelle.

På denne bakgrunnen fikk arbeidsgruppen følgende mandat:

Arbeidsgruppen skal:

- *Skaffe til veie oversikt over regelverk med betydning for informasjonssikkerheten.*
- *Peke på mulige problemområder med hensyn på mangler, overlappinger og/eller motstridigheter, samt etterlevbarhet av eksisterende regelverk. Brukere/regelverksforvaltere/tilsynsmyndigheter bør konsulteres.*
- *Utarbeide anbefalinger for hvordan de identifiserte problemområdene kan angripes på kort og lang sikt.*
- *Presentere resultatene/anbefalingene for KIS som drøfter videre oppfølging.*

Tid for ferdigstilling av forprosjektet:

*Prosjektet ferdigstilles og rapport avleveres KIS' sekretariat 3. juni 2005.
Resultatene og anbefalingene fra undergruppen presenteres for KIS på ekstraordinært medlemsmøtet den 21. juni 2005.*

2 Arbeidsgruppens sammensetning og arbeidsmetoder

KIS, i regi av Jan Tobiassen og Eivind Jahren, satt sammen følgende arbeidsgruppe:

- Amund Eriksen (leder), seniorrådgiver, cand.jur, Statskonsult
- Dag Wiese Schartum, professor dr. juris, Avdeling for forvaltningsinformatikk, Universitetet i Oslo (AFIN/UiO)
- Are Vegard Haug, stipendiat, Avdeling for forvaltningsinformatikk, Universitetet i Oslo (AFIN/UiO) (nå PHD-stipendiat, Institutt for statsvitenskap, UiO)
- Britt Jøsok, seniorrådgiver, cand. jur, Nasjonal sikkerhetsmyndighet (NSM)
- Kari Anne Lang-Ree, seniorrådgiver, cand. jur, Post- og teletilsynet (PT)
- Leif T. Aanensen, avdelingsdirektør, Datatilsynet (DT)
- Severin Vikanes, underdirektør, cand. jur, Forsvarsdepartementet (FD)
- Stig Ulstein, seniorrådgiver, Kredittilsynet (KT)
- Margaret Hagevik, seniorrådgiver, cand. jur, Statskonsult

I tillegg deltok Kirsti Berg, seniorrådgiver i Statskonsult i en startfase.

Her er e-postadresser og telefonnumre til arbeidsgruppen:

Deltaker	Organisasjon	e-post	telefon
Eriksen, Amund	Statskonsult	amund.eriksen@statskonsult.no	2245 1259
Haug, Are Vegard	Nå: Inst.for statsvitenskap, UiO	a.v.haug@stv.uio.no	2285 7675

Lang-Ree, Kari Anne	PT	kari-anne.lang-ree@npt.no	2282 4849
Schartum, Dag Wiese	AFIN/ UiO	d.w.schartum@jus.uio.no	2285 0077
Ulstein, Stig	Kredittilsynet	stig.ulstein@kredittilsynet.no	2293 9966
Vikanes, Severin	FD	severin.vikanes@fd.dep.no	2309 6151
Aanensen, Leif T.	Datatilsynet	leif.aanensen@datatilsynet.no	2239 6902
Britt Jøsok	NSM	bjosok@mil.no	6786 4121
Margaret Hagevik	Statskonsult	margaret.hagevik@statskonsult.no	2245 1141
Kirsti Berg	Statskonsult	kirsti.berg@statskonsult.no	2245 1127

2.1 Beskrivelse av arbeidsmåte og metode

Deltakerne i arbeidsgruppen ble endelig bestemt 8.mars 2005. Arbeidsgruppen hadde sitt første møte 31.mars. Det er holdt fem møter; fire tretimers møter og ett over to dager. Det har ikke vært mulig for alle å delta på alle møtene.

Deltakerne har lagt frem oversikter over emnet sett fra sine respektive sider, dels skriftlig og dels muntlig i møtene. En disposisjon til rapporten ble laget tidlig, og oppgaver fordelt. Møtene har vært arenaer for diskusjon. Mandatet forutsatte konsultasjon med regelverksforvaltere, tilsynsmyndigheter og brukere. Mange av de sentrale tilsynene har deltatt i arbeidsgruppen, samt en regelverksforvalter (FD). Øvrige forvaltere er det tatt kontakt med via de tilhørende tilsynsdeltakerne, for å få frem deres syn. Dette har fungert på et enkelt nivå. Brukere har arbeidsgruppen i liten grad hatt anledning til å konsultere i denne omgangen, innenfor de gitt tidsrammene. Mange av arbeidsgruppens deltakere har imidlertid betydelig kontakt med brukere i sitt arbeid, i egenskap av tilsyn.

2.1.1 Kunnskapsnettverk

På initiativ fra sekretariatsleder Jan Tobiassen i KIS ble det etablert såkalt "arbeidsrom" for arbeidsgruppen på nettsidene til www.kunnskapsnettverk.no. Ideen var at KIS skulle kunne fungere som styringsgruppe via dette opplegget, ved å få rask tilgang til de dokumentene arbeidsgruppen la ut på sine sider, som grunnlag for å følge med og gi sine synspunkter via de samme nettsidene.

Videre var ideen at Kunnskapsnettverket skulle effektivisere arbeidsgruppens måte å arbeide på, ved muligheten for rask publisering og tilgang til gruppens dokumenter.

2.2.2 Dokumentstudier

Arbeidsgruppen har nytt godt av de enkelte medlemmenes og andres til dels betydelige innsats på området informasjonssikkerhet og regelverk, som har funnet sted i annen regi. Det har vært et høyt aktivitetsnivå i den senere tid.

De følgende arbeidene er på mange måter mulig å betrakte som delvis oppfylld av arbeidsgruppens mandat (men uten at arbeidsgruppen står bak):

- *Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT*, Arild Jansen og Dag Wiese Schartum (red), Fagbokforlaget, 2005. Det er Avdeling for forvaltningsinformatikk (AFIN), UiO, der begge redaktørene er ansatt, som tok initiativet til denne utgivelsen. Boken gir i følge seg selv ”..den første og eneste samlede fremstillingen av regelverk om informasjonssikkerhet i Norge...” . Den gjennomgår noen av de mest sentrale regelverkene i forhold til informasjonssikkerhet. Syv regelverksområder fremstilles hver for seg, av ulike forfattere. I tillegg gis det en oversikt over utviklingstrekkene for rettslig regulering av informasjonssikkerhet, fra midten av forrige århundre til i dag. Dessuten gir boken oversikt over selve faget informasjonssikkerhet – informasjonssystemer, infrastrukturer og tekniske sikkerhetstiltak.

I et forord til boken skriver Moderniseringsminister Morten A. Meyer bl.a. følgende: ”*Jeg hilser velkommen det initiativet som her er tatt for å få en samlet gjennomgang av det viktigste sikkerhetsregelverket i Norge. Jeg tror denne boken kan være et nyttig hjelpemiddel i det daglige arbeidet med IT-sikkerheten og – ikke minst – et godt utgangspunkt for diskusjon om en samordning og forenklet etterlevelse av dette regelverket.*”

- *Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet?* Are Vegard Haug, Avdeling for forvaltningsinformatikk (AFIN), UiO 2005 (upublisert, under ferdigstilling pr mai 2005). Arbeidet er finansiert av Norges forskningsråd, og omtales av Haug som en ”underveisrapport” som må sees i en større sammenheng. Hans hovederend i rapporten er å prøve å etablere et forskningsmessig grunnlag for diskusjoner om lovregulering av informasjonssikkerhet, til nytte for brukere, produsenter av lover og forskrifter på området informasjonssikkerhet, og ikke minst til nytte for forskningsmiljøet.
- *Veiledning lover og regler med betydning for informasjonssikkerhet*, IT-SikkerhetsForum (ISF), versjon 1.1, september 2004. Veiledningen er utformet med sikte på å gi en oversikt over relevante lover og forskrifter som regulerer arbeidet med informasjonssikkerhet hos medlemmene av ISF. Den gir også en kort introduksjon til sikkerhetsbestemmelsene i utvalgte lover og forskrifter, men uten intensjon om å gi noen fullstendig beskrivelse verken av det enkelte regelverk eller hvordan kravene kan tilfredsstilles, enten kravene kommer fra ett eller flere regelverk. Selv om det primært er norske regler det gis oversikt over, er det også tatt med omtale av internasjonalt regelverk, samt veiledninger og annen nyttig informasjon.
- *Informasjonssikkerhet. Risikovurdering og sikkerhetsstyring – metoder og verktøy. En vurdering av egnethet for SMB*. En utredning for Nærings- og handelsdepartementet, av Johs. Hansen Hammer, 18.

august 2004. I tillegg til fokuset på kartlegging av standarder, veiledere, manualer, IT-baserte verktøy mv, har utredningen en kort gjennomgang av noen av de mest sentrale regelverkene med krav om informasjonssikkerhet, med kommentarer, og noen konkrete forslag til tiltak.

3 Oversikt over regelverk med betydning for informasjonssikkerhet

3.1 Kartlegging

En rekke lover og forskrifter stiller direkte eller indirekte krav til informasjonssikkerhet. Rettslig regulering kan også omfatte annet enn lover og forskrifter, for eksempel instruksjer og avtaler. Se omtale av ulike former for rettslige reguleringer i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*, kapittel 1.2. Bakerst i boken finnes en skjematisk oversikt over lover og forskrifter om informasjonssikkerhet.

Også andre har foretatt kartlegging av regelverk om informasjonssikkerhet. Oversikter finnes blant annet i følgende publikasjoner:

- Arild Jansen og Dag Wiese Schartum (red.): *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT* *Informasjonssikkerhet*
- IT-SikkerhetsForum: *Veiledning. Lover og regler med betydning for informasjonssikkerhet*
- *e-norge. Nasjonal strategi for informasjonssikkerhet*, juni 2003 (FD, NHD, JD)

Disse oversiktene viser at det er ulike syn på hva som bør betegnes som regelverk om informasjonssikkerhet.

I sin avhandling *Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet*, har forsker Are Vegard Haug foretatt en kartlegging av regelverket som omhandler informasjonssikkerhet. Kartleggingen innebærer en gjennomgang av de mest sentrale lovene og forskriftene som omhandler informasjonssikkerhet. Totalt er 34 regelverk gjennomgått, men det er også identifisert flere regelverk som omhandler informasjonssikkerhet. Med noen unntak har alle departementene egne lover og regler om informasjonssikkerhet. Dessuten er det mange regelverk som gjelder på tvers av samfunnssektorene. For hvert regelverk er det undersøkt hvilken ”regulatorisk strategi” som er valgt. Den regulatoriske strategien er operasjonalisert gjennom tre hovedtyper variabler med underpunkter: hovedregler, lovteknisk fremgangsmåte og virkemiddelbruk.

Se vedlegg 1.

3.2 Om bruk av standarder

Det henvises i liten grad til standarder. I henhold til forskrift 29.06.01 nr.723 om sikkerhetsadministrasjon § 4-2 om risikovurdering, kan myndighetene bestemme hvilken vurderingsmetode som skal benyttes.

Regelverk om informasjonssikkerhet er både generelt og detaljert utformet. Det synes ikke å være noe skille mellom at lover er generelle mens forskriftene er detaljerte. Mange forskrifter er til dels svært generelle, mens enkelte lover kan være detaljert utformet. De generelle kravene bygger på prinsipper om at den som skal etterleve regelverket selv må definere sikkerhetsnivået ut fra en egen risikovurdering. Brukerne av regelverket må derfor ha en form for internkontroll og kunne dokumentere overfor myndighetene at regelverkets krav er oppfylt. Som eksempler kan nevnes sikkerhetsregelverket, regelverket om personvern og regelverket om beredskap i kraftforsyningen.

Men for å etterleve regelverket vil brukeren ofte være hjulpet ved å benytte anerkjente standarder for sikkerhetsstyring og informasjonssikkerhet. NS-ISO/IEC 17799 Styringssystem for informasjonssikkerhet setter fokus på prosesser, snarere enn på krav til resultat. Denne standarden har påvirket forventninger til styringssystemer iht. personopplysningsloven, lov om helseregistre mfl. For enkelte virksomheter kan det bli for omfattende å følge prosessen etter NS 7799. Likevel vil man kunne få god veiledning ved å gjennomgå de viktigste elementene i standardens sikkerhetsopplegg.

Se Johs. H. Hammer: *Informasjonssikkerhet. Risikovurdering og sikkerhetsstyring – metoder og verktøy*, kapittel 5 og vedlegg 2, vedlegg 2.

3.3 Om gjennomføring av internasjonale regler – forpliktelser og føringer

En rekke av reglene om informasjonssikkerhet gjennomfører internasjonale forpliktelser. Den viktigste er EØS-avtalen. Også menneskerettighetene gir føringer når det gjelder rettsikkerhet i forhold til personvern og personopplysninger.

Lov om personopplysninger er ett eksempel på gjennomføring av internasjonale forpliktelser og brukes her som illustrasjon for hvilke forpliktelser og føringer som legges på norske myndigheter i denne sammenheng.

Det finnes forskjellige internasjonale regelsett som er av betydning for utformingen av norske regler om behandling av personopplysninger²:

- *Europarådets konvensjon 28 januar 1981 nr 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger ble ratifisert av Norge 20 februar 1984 og tok til å gjelde 1 oktober 1985.*
- *Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike*

² Se Ot.prp. nr.92 (1998-99) om lov om behandling av personopplysninger (personopplysningsloven).

opplysninger. Personverndirektivet bygger i utgangspunktet på prinsippene i Europarådets konvensjon om beskyttelse av personopplysninger, og forutsetter på enkelte punkter endringer i norsk lovgivning.

- Organisasjonen for økonomisk samarbeid og utvikling (OECD) utviklet i 1980 retningslinjer for beskyttelse og utveksling av persondata over landegrensene.
- Europarådets menneskerettskonvensjon 4 november 1950 og i FN-konvensjonen om sivile og politiske rettigheter av 1966 har artikler som har betydning for den enkeltes rett til privatliv og personlig integritet.
- NATO

De internasjonale forpliktelsene på dette området innebærer at det stilles minimumskrav til de nasjonale rettsreglene. Det betyr at reglene ellers kan utformes etter nasjonale normer for utforming av rettsregler.

Se også Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT. Direktiver og konvensjoner mv.* (vedlegg til boken) og ISF *Veiledning. Lover og regler med betydning for informasjonssikkerhet* vedlegg 5 til veiledningen.

3.4 Regler uten egen tilsynsmyndighet

Ansvar for regelverket ligger normalt i et departement. Det gjelder både lovene og forskriftene. I noen tilfelle er ansvaret for håndheving av regelverket delegert til et underliggende organ, for eksempel et tilsyn. Både regelverksansvaret og tilsynsansvaret innebærer å følge med på hvordan reglene virker. I praksis kan det imidlertid være en forskjell mellom ansvar og tilsyn. Dette blir tydelig der departementet ikke har delegert ansvaret for håndhevingen til et underliggende organ. Eksempler på slike regler er:

- Beskyttelsesinstruksen (SMK)³
- Offentlighetsloven (JD)
- Forvaltningsloven (JD)
- Forskrift om tingslysning (JD)
- Forskrift om registrering av juridiske personer m.m. i Enhetsregisteret (FIN)
- E-forvaltningsforskriften (MOD)
- Forskrift om registrering av foretak (NHD)
- Forskrift om petroleumregister (OED)

4 Noen erfaringer og mulige problemområder

4.1 Regelforvaltere

4.1.1 Moderniseringsdepartementet

³ Med unntak av bestemmelsene om elektronisk håndtering av informasjon gradert etter Beskyttelsesinstruksen, hvor NSM har fått myndighet til å gi råd og veiledning.

Ansvarsområde

Moderniseringsdepartementet forvalter

- Personopplysningsforskriften
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Erfaringer

Førstnevnte forskrift forvaltes i et samarbeid med Datatilsynet. Se kapittel 4.2.1 nedenfor om Datatilsynets nærmere fremstilling av personvernområdet og informasjonssikkerhet.

Se også artikkel skrevet av Dag Wiese Schartum *Krav til sikring av personopplysninger*, kapittel 5 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

Forskriften om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) ble først vedtatt med virkning fra 1.7.02 til 1.7.04. Hvis den ikke innen da ble fornyet, ville den "gå ned i solnedgangen" (opphøre). Dette var en forsiktighetsregel på et nytt og til dels pioneraktig område. Hensikten var å evaluere forskriften og se om det var grunnlag for å justere kursen, for en mer varig forskrift. Departementet gjennomførte slik evaluering, på grunnlag av kvantitative og kvalitative undersøkelser. Det ble observert en rekke erfaringer og problemområder, som tilsa til dels omfattende endringer særlig i forskriftens språk og redigering, for å gjøre den lettere forståelig. Innholdet ble i hovedtrekk beholdt, med noen få endringer.

Blant dem som svarte på den kvantitative spørreundersøkelsen, var det under 10 % av ansatte i kommunene som kjente forskriften, mot litt under 30 % i statsforvaltningen og litt under 40 % i fylkeskommunene. En typisk kommentar var: *Staten "glemmer" å introdusere forskriftene skikkelig overfor kommunesektoren.*

Gjennom undersøkelsen kom det mange kommentarer om at manglende kunnskap henger sammen med manglende informasjon, opplæring og kompetanse, f.eks. *Sikkert viktig å ha en slik forskrift. Men det hjelper så lite når en ikke har fått informasjon om at den finnes, og Ukjent, manglende informasjon om at den finnes, følges ikke opp av ansvarlig myndighet.* Blant dem som kjente den best, var arkivarer (43,6 %), mens ledere kjente foruroligende lite til den (14 %).

Se nærmere omtale i vedlegg 5: Evaluering av regelverk – ett eksempel. Sammendrag av rapport om evaluering av eForvaltningsforskriften, som Statskonsult gjennomførte på oppdrag fra Moderniseringsdepartementet.

Se også artikkel skrevet av Rolf Riisnæs *Sikker elektronisk samhandling med og i forvaltningen - eForvaltningsforskriften*, kapittel 7 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.1.2 Justisdepartementet

Justisdepartementet forvalter (bl.a.)

- Personopplysningsloven
- Forvaltningsloven
- Offentlighetsloven

Dette området er ikke nærmere beskrevet av arbeidsgruppen.

Se bl.a. artikkel skrevet av Dag Wiese Schartum *Krav til sikring av personopplysninger*, kapittel 5 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.1.3 Samferdselsdepartementet

Ansvarsområde

Departementet forvalter lov 04.07.03 nr 8 om elektronisk kommunikasjon (ekomloven). Med hjemmel i ekomloven har departementet fastsatt forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften).

Tilsynsansvar for sikkerhet og beredskap i elektroniske kommunikasjonsnett og tjenester er delegert til Post- og teletilsynet. Gjennom St.meld. nr. 47 (2000-2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* er tilsynet gitt ansvar for å vurdere og eventuelt iverksette ulike sikkerhetstiltak

Erfaringer

Sikkerhet i kommunikasjonsinfrastrukturen

Samferdselsdepartementet følger dette arbeidet gjennom ordinær rapportering fra Post- og teletilsynet. Ved bortfall av kommunikasjonstjenester og alvorlige brudd på sikkerheten blir departementet varslet.

Sårbarhet i Internett

Samferdselsdepartementet og Post- og teletilsynet følger utviklingen i bruk av Internett og vurderer fortløpende behovet for å implementere sikkerhets- og beredskapstiltak. Erfaringene så langt medfører at departementet ikke har sett behov for å iverksette noen spesifikke sikkerhetstiltak rettet mot ISPer⁴.

Departementet har satt i gang et arbeid for å utrede behovet for en eventuell regulering på dette området.

Bevisstgjøring, kompetansehevning og veiledning

Samferdselsdepartementet er opptatt av at IKT-sikkerhet blir diskutert og satt på dagsorden i ulike sammenhenger, og har i dialog med Moderniseringsdepartementet og Post- og teletilsynet løftet IKT-sikkerhet som

⁴ ISP-er er omfattet av ekomloven og har en plikt til å registrere seg som tilbydere av en tjeneste.

tema. Lanseringen av nettstedet *Nettvett.no* er et viktig tiltak for å veilede brukere av elektronisk kommunikasjon om sikkerhet.

Generelle utfordringer

En generell utfordring når det gjelder IKT-sikkerhet og regelverk er at krav til sikkerhet vil kunne komme i konflikt med ønsket om innovasjon og konkurranse. For strenge krav til sikkerhet kan være en begrensning i forhold til utvikling i teknologi og marked.

Mye tyder på at behovet for harmonisering av regelverk innenfor EU/EØS-området når det gjelder IKT-sikkerhet øker. Per i dag stilles det ulike krav til sikkerhet overfor tilbyderne av elektroniske kommunikasjonsnett- og tjenester i de ulike landene, og tilbydere som opererer i flere land reagerer negativt på ulike rammevilkår.

Bestemmelser i ekomloven og ekomforskriften

Når det gjelder de enkelte bestemmelsene om sikkerhet i ekomloven og ekomforskriften er det ikke påpekt noen store svakheter ved disse.

Lovbestemmelsene er generelle og omfatter alle aspekter ved sikkerhet (tilgjengelighet, integritet og konfidensialitet). Fra tilbyderne har det blitt påpekt som en svakhet at det er uklart hvilket nivå for sikring som legges til grunn.

Forholdet til andre lover

Ekomloven supplerer sikkerhetsloven og overlapper delvis.

4.1.4 Forsvarsdepartementet

Ansvarsområde

Departementet har et overordnet ansvar for forebyggende sikkerhetstjeneste i militær sektor. Ansvaret for gjennomføring av de forebyggende sikkerhetstiltak følger av lov 20.03.1998 nr 10 om forebyggende sikkerhet (sikkerhetsloven) § 4 første ledd og § 5 første ledd. Lovens virkeområde er stats- og kommuneforvaltningen, samt private virksomheter som er leverandører av varer eller tjenester til det offentlige i forbindelse med sikkerhetsgraderte anskaffelser. Departementet har flere ganger utvidet lovens virkeområde.

Sikkerhetsloven gjelder i forhold til både skjermingsverdig informasjon og objekt, uavhengig av om det befinner seg i militær eller sivil sektor.⁵ Tradisjonelt har konsekvenser knyttet til rikets sikkerhet blitt forbundet med det *ytre forsvar* og dermed til militæret og diplomatiet. Med samfunnsutviklingen har dette endret seg. Dette kommer også til uttrykk ved at formålet med sikkerhetsloven er å beskytte rikets selvstendighet og sikkerhet, i tillegg til *andre vitale nasjonale sikkerhetsinteresser*. Problemstillingene blir dermed aktuelle for alle samfunnssektorer.

⁵ Ansvaret for sikkerhetstjeneste i sivil sektor er imidlertid tillagt Justisdepartementet.

Regjeringens kontroll med den forebyggende sikkerhetstjenesten utøves gjennom Nasjonal sikkerhetsmyndighet (NSM) og ved Forsvarsdepartementets kontroller med NSM⁶.

Erfaringer

Risikobegrepet i sikkerhetsloven omfatter både planlagte hendelser og mer tilfeldige hendelser med utilsiktede konsekvenser. Bedømming av risiko må være basert på informasjon fra etterretning⁷ og statistikk⁸. Sikkerhetstiltak mot ikke-villede hendelser er i stor grad regulert gjennom sektorlovgivningen. Det synes imidlertid ikke å foreligge noen mekanismer som sikrer en felles oppfatning av risikobildet som skal ligge til grunn for utvikling av sikkerhetstiltak under sikkerhetsloven og sektorlovgivningen. Sikkerhetsloven er heller ikke i særlig grad samordnet med sektorlovgivningen.

Forskriftsverket under sikkerhetsloven er meget detaljert. Det gjør sikkerhetsregimet lite dynamisk i forhold til den teknologiske utvikling. Videre blir det vanskelig ut fra helhetlige risikovurderinger å avstemme behovet for konfidensialitet i forhold til tilgjengelighet og effektivitet. Forskrift om informasjonssikkerhet bygger blant annet på fysisk sikring av områder hvor det skal håndteres gradert informasjon. Det skaper blant annet vanskeligheter i forhold til samfunnets behov for mobile løsninger.

4.2 Tilsynsmyndigheter

I tabellen nedenfor er det listet opp tilsynsmyndigheter med ansvar for informasjonssikkerhet. Listen er ikke komplett, men illustrerer at det er mange myndigheter som er inne i bildet.⁹

Tilsynsmyndighet	Lover og forskrifter som gir hjemmel for tilsynet
Rikstrygdeverket	- Lov om folketrygd (folketrygdloven)
Markedsrådet og Forbrukerombudet	- Markedsføringsloven
Kommunene	- Barnehageloven
Kredittilsynet	- IKT-forskriften og internkontrollforskriften (for finansinst.)
Tollvesenet	- Tollloven
Skattedirektoratet (Datatilsynet)	- Forskrift om elektronisk tilgang til opplysninger i ligningsforvaltningens registre
Datatilsynet, Fiskeridirektoratet	- Forskrift om lagring av satellittopplysninger
NSM	- Sikkerhetsloven
	- Forskrift om informasjonssikkerhet
	- Forskrift om sikkerhetsadministrasjon
	- Forskrift om sikkerhetsgraderte anskaffelse
	- Forskrift om personellsikkerhet
Helsetilsynet (Datatilsynet)	- Helseregisterloven
	- Reseptregisteret
	- MSIS- og Tuberkuloseregisterforskriften
	- Forskrift om pasientjournaler

⁶ Jf. forskrift 04.07.03 nr 900 om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.

⁷ Spionasje, sabotasje og terrorhandlinger - og relevante intensjonsbaserte handlinger med annet formål.

⁸ Menneskelig, rutinemessig og teknisk svikt - og naturskade.

⁹ Kilde: Are Vegard Haug: Rettslige reguleringer av informasjonssikkerhet.

Datatilsynet	- Personopplysningsloven - Personopplysningsforskriften - SIS-loven - Forskrift om føring av grunneiendoms-, adresse- og bygningsregisteret (GAB- registeret)
Post- og teletilsynet, (Datatilsynet)	- Esignaturloven - Forskrift om krav til utsteder av kvalifiserte sertifikater mv. - ekomloven - ekomforskriften - Domeneforskriften
Norges vassdrag og elektrisitetsvesen	- Forskrift om beredskap i kraftforsyningen

I det følgende beskrives erfaringer fra noen utvalgte tilsynsmyndigheter.

4.2.1 Datatilsynet

Tilsyn

Datatilsynet skal kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger overholdes. Det gjennomføres årlig mellom 100-150 tilsyn, herunder kontroll av informasjonssikkerhet.

Datatilsynet har myndighet til å fastlegge særskilte kriterier for akseptabelt risikonivå og å fastlegge spesielle vilkår for sikkerhet ved behandling av personopplysninger. Tilsynet kan også overprøve behandlingsansvarliges vurderinger, for eksempel i forbindelse med tilsynsaktiviteter.

Datatilsynet fører tilsyn med følgende regelverk:

- Lov om personopplysninger § 13
- Forskrift om personopplysninger kapittel 2

Regelverket bygger på prinsippet om forholdsmessig sikring av personopplysninger og at det er behandlingsansvarlig som er best egnet til å vurdere hvordan opplysningene skal sikres. Behandlingsansvarlig må derfor kunne vise til at slike vurderinger er gjort og at valgene som er foretatt er forsvarlig (internkontroll).

Erfaringer

Enkelte virksomheter var svært gode på personvern og informasjonssikkerhet. Men de fleste manglet systematikk, mange overholdt ikke sletteplikt og hadde dårlig sikkerhet ved elektronisk samhandling.

Mange aktører har fortsatt manglende kunnskap om regelverket. Dette synliggjøres i første rekke gjennom at virksomhetene ikke har etablert en oversikt over hvilke personopplysninger de faktisk behandler. De har heller ikke satt i gang nødvendige aktiviteter for å møte de pliktene de har i følge regelverket. De aller fleste tilsynsobjektene får derfor anmerkning fra Datatilsynet om manglende internkontroll. Dette er alvorlig fordi internkontrollsystemet, og tilhørende bestemmelser om

*informasjonssikkerhet, skal danne fundamentet i etterlevelsen av personvernlovgivningen.*¹⁰

Virksomhetene synes å slite med å:

- sette rammer for arbeidet med informasjonssikkerhet
- etablere en tilfredsstillende systematikk
- utarbeide risikovurdering
- ha oversikt over informasjonssystemet
- ivareta sikker samhandling med andre
- iverksette tilstrekkelige tiltak

Se også artikkel skrevet av Dag Wiese Schartum *Krav til sikring av personopplysninger*, kapittel 5 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.2.2 Post- og teletilsynet

Tilsyn

Post- og teletilsynets (PT) hovedansvarsområde er å regulere og overvåke sektoren for elektronisk kommunikasjon i Norge. PT forvalter flere begrensede ressurser, foretar markedskontroll av utstyr, bidrar til økt teleberedskap og sikkerhet, har ansvaret for telestandardisering og driver rådgivning overfor Samferdselsdepartementet. Post- og teletilsynet fører tilsyn med at følgende regelverk blir etterlevd:

- Lov 04.07.03 nr. 83 om elektronisk kommunikasjon av ([ekomloven](#)), §§ 2-3, 27, 2-10 gjelder informasjonssikkerhet
- Forskrift 16.02.04 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste av ([ekomforskriften](#)).
- Lov 15.06.01 nr. 81 om elektronisk signatur av ([esignaturloven](#)) regulerer aspekter av sikkerhet innen domeneforvaltning.
- Forskrift 15.06.01 nr 661 om krav til utstedere av kvalifiserte sertifikater mv. av ([esignaturforskriften](#))
- Forskrift 01.08.03 nr. 990 om tildeling av domenenavn under norske landkodedetopdomener av ([domeneforskriften](#)) regulerer aspekter av sikkerhet innen domeneforvaltning

Erfaringer

Tilsyn med sikkerhet og beredskap i nett

PT skal påse at grunnleggende kommunikasjonstjenester har et sikkerhetsmessig tilfredsstillende nivå. Videre skal PT påse at viktige samfunnsinstitusjoner og tilbydere har beredskapsplaner og rutiner for håndtering av unormale situasjoner, herunder situasjoner med ekstreme kommunikasjonsbehov. PT arrangerer og koordinerer øvelser hvert annet år for å trene operatørene i å samarbeide for å håndtere slike situasjoner best mulig.

¹⁰ Fra Datatilsynets rapport 2004. se http://www.datatilsynet.no/templates/Page_1008.aspx

Samarbeidet kan være mellom operatørene eller for eksempel mellom operatører og kraftleverandør.

Følgende eksempler illustrerer PTs tilsynsvirksomhet på dette området:

- Ekom-aktørene har plikt til å rapportere om større problemer og uhell til PT. Ved behov utfører PT stedlig tilsyn hos operatørene.
- Det gis offentlig tilskudd til bygging og drift av fjellanlegg som rommer vitalt utstyr for nettenes funksjon. Det gis også støtte til innkjøp av reservemateriell. PT har i samarbeid med operatørene deltatt i kontroll av slike sikrede anlegg.

Tilsyn med utstedere av kvalifiserte sertifikater

Tilsynsarbeidet er lagt opp etter en selvdeklarasjonsmodell. Den som ønsker å utstede sertifikater må registrere seg hos PT og oversende sertifikatpolicy og sertifikatpraksis. PT gjennomgår de registrerte opplysningene, sammenholder dem med krav i lov og forskrift og ber om tilleggsopplysninger etter behov. PT kan også foreta stedlig tilsyn og kreve at tilbyderen gjennomfører IT-revisjon.

PTs erfaringsmateriale er begrenset. Inntil nylig var det kun registrert én utsteder av kvalifiserte sertifikater. Dette er et nytt tilsynsområde med ny lovregulering og det foreligger ikke relevant praksis eller autoritativ tolking av lovverket. Problemer som den første utstederen har opplevd er i stor grad er knyttet til det faktum at de må pløye ny mark.

Tilsyn med NORID

PT har en god dialog med Norid¹¹. Grunnet monopolsituasjonen er det vanskelig å bruke tilsynserfaringene fra dette området i andre sammenhenger. Domeneforskriften er en relativt ny forskrift som skal evalueres i 2005. Det vil det først og fremst være klageordningen som skal evalueres. Så langt er det ikke oppdaget konfliktområder mellom domeneforskriften og annet regelverk.

Selvregulering

Selvregulering er et viktig virkemiddel for å oppnå samarbeid og løse problemer på en rask måte uten å måtte bruke lovregulering. PT opprettet i 1997 *Nummergruppen* - en uformell møteplass for tilsynet og teleaktørene.

PT også etablert en Internettgruppe og undergruppen ABUSE, som har fokus på misbruk av kommunikasjonen over nettet. Begge grupper består av representanter både fra myndighetene og aktørene og diskuterer regulatoriske, tekniske og kommersielle aspekter.

Veiledning og informasjon

Nettstedene *Telepriser.no*, *Bredbåndsporten.no* og *Nettvett.no* inneholder informasjon rettet mot forbrukere og bedrifter.

Samarbeid mellom tilsyn

¹¹ **Registerenhet for det norske toppdomenet .no. Norid er i en nødvendig monopolsituasjon da det av praktiske og tekniske grunner er mulig med kun én registerenhet for det enkelte toppdomenet.**

PT har inngått avtaler om uformelt samarbeid med Konkurransetilsynet og forbrukermyndighetene. Tilsynet vurderer nå å formalisere et samarbeid med Datatilsynet. PT fører også samtaler med Kredittilsynet for å forberede en kommende registrering av bankene som utstedere av kvalifiserte sertifikater. Bankene er underlagt omfattende tilsyn fra Kredittilsynet, mens PT vil føre tilsyn med begrensede deler av bankenes virksomhet.

4.2.3 Kredittilsynet

Tilsyn

Kredittilsynet fører tilsyn med forskrift 16.12.92 nr. 1157 om bruk av informasjonsteknologi (IT-forskriften). Forskriften gjelder for norske forretningsbanker, sparebanker, livs-/skadeforsikringsselskaper, Bankenes Betalingsentral, Verdipapirsentralen, oppgjørssentral iht. verdipapirhandelsloven kapittel 6 og børser og autoriserte markedsplasser iht. børsloven § 3-4 første ledd, annet punkt. Forskriften omfatter foretakets IT-systemer for rapportering i samsvar med gjeldende lover og forskrifter, og systemer for øvrig som behandler økonomisk informasjon av viktighet for styring og kontroll.

Det føres også tilsyn med forskrift 20.06.97 nr. 1057 om klargjøring av kontrollansvar, dokumentasjon og bekreftelse av den interne kontroll (forskrift om internkontroll, finansinstitusjoner). Forskriftens virkeområde gjelder tilsvarende som for IT-forskriften (se avsnitt ovenfor).

Erfaringer

I 2001 startet Kredittilsynet arbeidet med å utvikle en ny tilsynsmetode for IT-tilsynet. Denne ble basert på en internasjonal metode med betegnelsen CobiT (Control Objectives for Information and Related Technology) administrert og videreutviklet av den brukerstyrte internasjonale medlemsorganisasjonen ISACA (Information Systems Audit and Control Association). Denne organisasjonens hovedaktivitetsområde er knyttet til arbeid med IKT-styrings-, kvalitetssikrings- og IKT-revisjonsarbeid.

Metoden er prosessbasert og inndeler alle IKT-prosesser inn i 4 hovedområdene; Planlegging og organisering, som omfatter 11 prosesser, Anskaffelse og implementering som omfatter 6 prosesser, Leveranse og støtte som omfatter 13 prosesser og Overvåking som omfatter 4 prosesser. Samlet utgjør dette 34 IKT-prosesser. Den prosessorienterte tenkningen baserer seg på forutsetningen om at foretaket må ha etablert en definert prosess for å kunne ivareta de ulike IT-oppgavene. Basert på at metoden dermed dekker hele IKT-virksomheten til et foretak, har Kredittilsynet utviklet kontrollspørsmål knyttet til den enkelte prosess, på laveste nivå. Knyttet til de 34 IKT-prosessene som er definert i metoden har vi utviklet ca 180 kontrollspørsmål som er relatert til den enkelte IKT-prosess. I tillegg til at foretakene svarer på disse spørsmålene og returnere disse til Kredittilsynet, bes det om et fast utvalg av dokumenter som skal understøtte de svar som er avgitt. Metoden baserer seg på risikotenkning og at det er de forretningsmessige mål som i stor grad vil styre omfanget av det sikkerhetsregime som foretaket skal ha etablert.

Resultatene som Kredittilsynet har fått gjennom bruken av metoden vurderes å være svært gode. Vi har gjennomført ca 100 IT-tilsyn over denne perioden. Erfaringen fra metodebruken har til en viss grad farget arbeidet med den nye IKT-forskriften slik at denne i noe grad følger prosesstenkningen som CoBIT legger til grunn i sitt rammeverk. Enkelte viktige IKT-prosesser finnes derfor som egne bestemmelser i forskriften. Dette gjør at det kan utvikles et samspill mellom IT-tilsynsaktivitetene og samtidig avsjekking av hvordan foretaket ivaretar kravene i forskriften.

Veiledning og informasjon

Det er utarbeidet veiledninger til IT-forskriften.

Se også Frank Robert Berg *Informasjonssikkerhet i finansnæringen – IKT-forskriften*, kapittel 8 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.2.4 Nasjonal sikkerhetsmyndighet (NSM)

Tilsyn

NSM driver kontrollbasert tilsyn av sikkerhetstilstanden i stats- og kommuneforvaltningen og i private virksomheter som er leverandører av varer eller tjenester til det offentlige i forbindelse med sikkerhetsgraderte anskaffelser.

Ansvar for sikkerheten er forankret i departementene. Det er derfor ønskelig å se nærmere på hvilke føringer de har gitt sine underlagte virksomheter, hvilke krav de stiller til rapportering for å skaffe seg oversikt og hvilke tiltak de iverksetter for å sikre at kravene i sikkerhetsloven med forskrifter blir fulgt opp. På denne bakgrunn er man i ferd med å gå over til et mer dokumentasjonsbasert tilsyn med overordnede virksomheter. NSM vil fortsatt kontrollere at nødvendige tiltak er implementert både i departementer og underliggende virksomheter.

NSM fører tilsyn med følgende regelverk:

- Lov 20.03.1998 nr 10 om forebyggende sikkerhet (sikkerhetsloven)
- Forskrift 29.06.01 nr. 0723 om sikkerhetsadministrasjon
- Forskrift 01.07.01 nr.744 om informasjonssikkerhet
- Forskrift 29.06.01 nr.722 om personellsikkerhet
- Forskrift 01.07.01 nr.753 om sikkerhetsgraderte anskaffelser
- Forskrift 17.03.72 nr.3352 (beskyttelsesinstruksen) vedrørende elektronisk lagring av gradert informasjon (råd og veiledning) ¹²

Veiledning og informasjon

NSM har gjennomført følgende tiltak:

- sikkerhetskonferanser for kommuner og fylkeskommuner

¹² Statsministerens kontor har det formelle ansvaret for BI

- undervisningsvirksomhet ved både sivile og militære kurs- og utdanningsinstitusjoner
- årlig en sikkerhetskonferanse
- helpdesk-telefoner for å bistå brukerne ved eventuelle problemer knyttet til bruk av krypto eller ved sikkerhetsklarering av personell.

NSM har utarbeidet ulike veiledninger til regelverket. Disse blir jevnlig oppdatert og formidlet blant annet gjennom NSMs hjemmeside. NSM kjenner ikke til at er det ikke gitt noe veiledning til beskyttelsesinstruksen.

Erfaringer

Svakheter ved regelverket

Forsvarsdepartementet kan utvide sikkerhetslovens virkeområde ved å bestemme at hele eller deler av sikkerhetsloven skal gjelde for enkeltpersoner, foreninger, stiftelser, selskaper og privat og offentlig næringsvirksomhet *som mottar sikkergradert informasjon fra et forvaltningsorgan*.¹³ Kompetansen er således begrenset ved at man ikke kan fange opp alle virksomheter som produserer skjermingsverdig informasjon. I praksis driver mange virksomheter personkontroll uten hjemmel, noe som innebærer et rettsikkerhetsproblem. Begrensningene er også problematisk i forhold til Norges internasjonale forpliktelser.

Sikkerhetsloven inneholder minimumskrav og bygger ikke på prinsippet om forholdsmessig beskyttelse av skjermingsverdig informasjon. Det forventes imidlertid at tiltakene skjerpes dersom situasjonen endrer seg og trusselnivået blir høyere. Mangelen på forholdsmessighet kan være problematisk for virksomheter som bare har skjermingsverdig informasjon i et begrenset omfang. Videre kan det være et problem at loven har ensidig fokus på konfidensialitetsaspektet, og åpner ikke for at hensynet til tilgjengelighet eller integritet skal kunne ha betydning i forhold til hvilke krav som stilles til sikkerhetstiltak.

Sikkerhetsadministrasjon

NSM har registrert avvik fra kravene i forskrift om sikkerhetsadministrasjon, blant annet:

- internkontroll, herunder mangel på evaluering av egen sikkerhetstilstand
- organisering av sikkerheten, herunder ansvars plassering, forankring i ledelsen og tilgjengelige ressurser
- rapportering av sikkerhetstruende hendelser

Informasjonssystemssikkerhet

NSM har registrert avvik fra kravene i forskrift om informasjonssikkerhet, blant annet:

- manglende sikkerhetsgodkjenning på systemer som behandler gradert informasjon

Beskyttelsesinstruksen

¹³ Sikkerhetsloven § 2, 1. ledd, 3. pkt

NSM ser at det er noe usikkerhet knyttet til bruk av Beskyttelsesinstruksen (BI), og at ansvarsforholdene her er uklare for de virksomhetene som skal bruke den.

Generelt

Internt i NSM er det grunn til å tro at det liten kunnskap om, og/eller fokus på, andre nasjonale sikkerhetsregelverk en virksomhet står overfor. Virksomhetene står derfor alene i forhold til å samordne kravene fra de ulike tilsynsmyndighetene og sikkerhetsregelverkene.¹⁴

Se også artikkel skrevet av Amund Eriksen *Sikkerhetsloven og informasjonssikkerhet*, kapittel 9 i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.2.5 Norges vassdrags- og energidirektorat (NVE)¹⁵

Tilsyn

I fred skal NVE, som beredskapsmyndighet, samordne beredskapsplanleggingen i kraftforsyningen. En regional og nasjonal rasjoneringsberedskap skal håndteres av Kraftforsyningens beredskapsorganisasjon (KBO). Vedtak om sikringstiltak ved kraftforsyningsanlegg kan treffes for bestående anlegg, anlegg under bygging eller planlagte anlegg som er eller trolig vil bli av betydning for landets kraftforsyning. Olje- og energidepartementet kan fastsette en bestemt frist for gjennomføringen av pålegg og en daglig løpende tvangsmulkt ved oversittelse av fristen. Blir pålegget ikke etterkommet kan departementet la pålegget utføres på vedkommendes bekostning.

NVE fører tilsyn med forskrift 12.16.02 nr 1606 om beredskap i kraftforsyningen. Kapittel 6 omhandler informasjonssikkerhet. NVE har utarbeidet veiledning til forskriften.

Erfaringer

Forskriften setter krav til beredskapsplaner, funksjoner og overordede mål fremfor detaljer. Alle anlegg klassifiseres av NVE, avhengig av anleggets viktighet. Virksomheten står fritt til å velge hvilke sikringstiltak som skal iverksettes på bakgrunn av virksomhetens egen risiko- og sårbarhetsanalyse som utføres på bakgrunn av de krav som er knyttet til anleggets klasse. Kravene i forskriften skal integreres i virksomhetens kvalitetssystem, som skal ivareta både virksomhetenes og tilsynsmyndighetenes behov for kontroll og dokumentasjon.

Etter hvert som offentlig virksomhet setter ut tjenester på anbud, må det nøye spesifiseres de krav som settes til tjenesten. Dette har allerede kraftforsyningen holdt på med i noen år.

¹⁴ Arbeidsgruppen mener det er grunn til å anta at dette gjelder de fleste tilsynene.

¹⁵ Informasjon er gitt av Carl Georg Abel i NVE

Våre erfaringer fra tilsyn, er en stor imøtekommenhet fra bransjen. Men det er åpenbare prinsipielle problemstillinger. For eksempel kan man, av økonomiske hensyn, la være å opplyse om forhold som ikke er ”bra nok”, fordi et pålegg fra myndighetene nødvendigvis vil koste penger, og ikke generere tilsvarende inntekter.

Nettleverandører og leverandører av kraft må forholde seg til mange forskjellige lover og forskrifter om informasjonssikkerhet. Reglene har til dels ulik tilnærming, noe som kan være problematisk for etterlevelse.

For å illustrere omfanget av regelverk som nettleverandører må forholde seg til, vises det til oversikt utarbeidet av Statnett. Oversikten følger som vedlegg...

4.3 Noen brukersynspunkter

For dette prosjektet ikke vi ikke hatt mulighet til selv å gjennomføre intervjuer med brukergrupper. Rapporten støtter seg derfor blant annet på intervjuer som er gjennomført i forbindelse med et annet prosjekt om informasjonssikkerhet i forvaltningen¹⁶. Informantene fikk blant annet spørsmål om hvilke kunnskaper de hadde om regelverk knyttet til informasjonssikkerhet.

I sammenfatning og sammendrag fra møter med kommunal sektor¹⁷ heter det blant annet:

- *De mange lover, forskrifter og regler skaper et uoversiktlig ”landskapsbilde” for personer som skal stelle med ”hverdagsikkerheten”, ofte som en tilleggsaktivitet til andre oppgaver. I dag overskues dette bare av juristene. Det er derfor nødvendig å få på plass en struktur og oversikt på dette området.*
- *Det er behov for en koordinert tverrsektoriell innsats for å rydde opp og gjøre det enklere for kommuner og fylkeskommuner å forholde seg på en strukturert måte til de ulike delene av regelverket.*
- *Det er behov for veiledning om praktisk gjennomføring av lover og forskrifter vedrørende informasjonssikkerhet innen de enkelte ansvarsområder.*
- *Regelverket må brukes og respekteres også av departementene, det er snakk om liv og lære!*

Statens pensjonskasse har både elektroniske publikumstjenester og intern elektronisk saksbehandling. En informant fra Statens pensjonskasse har gitt uttrykk for at det er behov for en samlet fremstilling av regelverket for informasjonssikkerhet, ikke ved endring av regelverket, men ved en utvikling av veiledninger.

Synspunkter fra brukerne gir seg også uttrykk gjennom uttalelse fra IT-SikkerhetsForum. De skriver blant annet¹⁸:

¹⁶ Prosjektet utføres av Statskonsult på oppdrag fra Moderniseringsdepartementet.

¹⁷ Statskonsult, internt prosjektnotat 10.12.04

En stor utfordring for norske virksomheter er at mange av dem omfattes av flere regelverk. Eksempelvis vil virksomheter innen finanssektoren være pålagt sikkerhetsbestemmelser både fra Personopplysningsloven og Kredittilsynets IT-forskrift; i tillegg vil de også kunne bli underlagt bestemmelser i Sikkerhetsloven, som følge av ny forskrift om objektsikkerhet – en del av kritisk infrastruktur. Regelverkene er ofte bygget opp på en uensartet måte. Noen har mer fokus på tekniske tiltak og andre på arbeidsprosessen, og de kan understøtte ulike sikkerhetsfaglige tilnæringsmåter til arbeidet. Så lenge regelverkene ikke koordineres der de utvikles, må koordinering skje der reglene etterleves – det vil si i den enkelte virksomhet. Målsettingen for virksomhetene bør/må uansett være å etablere én sikkerhetsløsning som tilfredsstillende flere/alle lovmessige sikkerhetskrav, i tillegg til de forretningsmessige og kontraktuelle kravene.

4.4 Problembeskrivelse – analyse og vurderinger

4.4.1 Innledning

Punkt 4.4.4 er i sin helhet skrevet av forsker Are Vegard Haug og er hentet fra rapporten *Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet*. Hans analyser og vurderinger er nærmere utdypet og fremgår av vedlegg 4.

4.4.2 Analysemetode

For å kunne identifisere reglernes innhold og hvem de gjelder for, kan det være nyttig å dele dem inn i kategorier. En nærmere kategorisering kan være nyttig for myndighetene for å vurdere muligheter for forbedringer. For brukerne kan kategoriseringen være nyttig i forbindelse med risikovurderingen og etterlevelse av reglene.

Kategorisering av regelverket etter sikkerhetsnivå

- Regler som gjelder alminnelig sikkerhet under vanlige samfunnsforhold: (regelverk om personopplysninger, regelverk om beredskap i kraftforsyningen, ekomregelverket m.v.)
- Regler som gjelder rikets sikkerhet og sikkerhet for kritiske funksjoner og situasjoner (sikkerhetsloven med forskrifter og regelverk om beredskap i kraftforsyningen m.v..)

Kategorisering av regelverket etter virkeområde og ansvar for håndheving

- Hva omfattes av reglene (detaljregler og funksjonskrav)
- Hvem retter reglene seg mot (plikter for myndighetene ((skal kontrollere.. osv.) alle offentlige og private virksomheter, enkelte bransjer)
- Hvem har ansvar for håndheving av reglene (regelverksansvarlig der det ikke er en tilsynsmyndighet, for eksempel e-forvaltningsforskriften (MOD) og tilsynsansvarlig (Datatilsynet, Kredittilsynet osv.))

¹⁸ Veiledning. Lover og regler med betydning for informasjonssikkerhet, 2003.

4.4.3 Tidligere studier som omhandler regelverk om informasjonssikkerhet (offentlige utredninger og evalueringer)

I dette prosjektet har vi benyttet oss av ulike studier på området. Studiene viser at det er reist ulike typer kritikk av de rettslige virkemidlene som brukes for å skape informasjonssikkerhet. En type kritikk dreier seg om at lovgivningen er fragmentert. Det hevdes at det er vanskelig å finne ut hva "regelen" egentlig er, fordi den er spredt i ulike lover, forskrifter, instruksjoner og andre rettskilder.

En annen type kritikk handler om at rettsreglene har økt i volum og omfang, og slik sett bidratt til et unødvendig byråkrati og skapt juridiske barrierer. Eksempler som typisk trekkes frem er uklare roller, omfattende krav som er vanskelig å etterleve, mange tilsynsorgan, osv. Mange sikkerhetsregelverk gjelder for en og samme virksomhet. Som eksempel har Statsnett for sin del utarbeidet en oversikt hvilke regler som gjelder for nettleverandører. Oversikten viser at Statsnett må forholde seg til 13 lover og forskrifter og et antall ulike tilsynsmyndigheter. Se vedlegg 3.

Gjennom årene har myndighetene nedsatt en rekke utvalg. Seip-utvalget¹⁹, Styrings- og arbeidsgruppene for samordning av regelverk for beskyttelse av informasjon²⁰ og Willoch-utvalget²¹ står sentralt i denne sammenheng.

Se også artikkel skrevet av Amund Eriksen *Rettsregler og informasjonssikkerhet – noen utviklingstrekk*, kapittel 2 (jf bl.a. kap. 2.6, 2.7, 2.8, 2.10 og 2.11) i Arild Jansen og Dag Wiese Schartum (red.) *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Fagbokforlaget 2005.

4.4.4 Analyse og vurdering av de rettslige reguleringene av informasjonssikkerhet

Ulike teknikker for å avgrense reglens virkeområde

Gjennomgang av regelverkene viser at det brukes mange forskjellige teknikker for å avgrense reglens virkeområde. Det ble påvist 6 ulike teknikker for å avgrense saklig virkeområde: *lovstyrt, foretaksstyrt, opplysningstypestyrt, behandlingsstyrt, formålstyrt og ekstern avgrensing*. Noen av teknikkene er så indirekte og vanskelige å anvende at det kan medføre at brukerne i utgangspunktet ikke finner ut om regelverkene gjelder for dem eller ikke. Når det gjelder geografisk virkeområde finnes det stort sett enkle bestemmelser som slår fast at reglene gjelder i Norge. Det finnes riktignok unntak, for eksempel personopplysningsloven med forskrift, men dette er likevel nokså avgrensede forsøk på å løse de mer fundamentale problemene for sikkerheten som følger av (særlig) Internettets globale karakter. Effekten av nasjonal lovgivning er på

¹⁹ NOU 1986:12 Datateknikk og samfunnets sårbarhet

²⁰ Rapport fra en arbeidsgruppe nedsatt av Forsvarsdepartementet, Justisdepartementet, og Arbeids- og administrasjonsdepartementet, desember 1991: Samordning av regelverk for beskyttelse av informasjon.

²¹ NOU 2000:24 Et sårbart samfunn. utfordringer for sikkerhets og beredskapsarbeid i samfunnet

dette området nokså begrenset, og illustrerer behovet for internasjonal koordinert lovgivning.

Overlappning og manglende koordinering

Det er mange og til dels sterke overlappinger og manglende koordinering av regelverkene om informasjonssikkerhet. Antall regler er omfattende og mange virksomheter må forholde seg til flere regler om informasjonssikkerhet samtidig. Gjennomgangen viser at omfanget spenner fra helt enkle situasjoner, der bare personopplysningsloven gjelder, til situasjoner hvor et titalls regelverk får anvendelse på samme tid. Den første situasjonen oppstår hos enkle private virksomheter med marginal behandling av personopplysninger. Den siste situasjonen oppstår i forvaltningen dersom det for eksempel behandles opplysninger som både er personopplysninger og helseopplysninger på samme tid (ved bruk av elektronisk signatur og at det påligger etaten et beredskapsansvar som inkluderer beskyttelse av *skjermverdig* informasjon). Men også for næringslivet ser vi at mange regelverk kommer til anvendelse på samme tid. Det mest ekstreme tilfellet er norske primærkommuner som i kraft av sitt generelle funksjonsområde antakelig må forholde seg samtidig til opp mot 20 regelverk som omhandler informasjonssikkerhet.

Det vil imidlertid være langt mer vanlig at private og offentlige virksomheter forholder seg til færre regelverk, i det daglige kanskje 3 -5 regelverk om informasjonssikkerhet på samme tid. Og selv om antall regler er omfattende er det funnet få (om noen) eksempler på direkte motstrid. De enkelte regulatoriske tiltakene er nokså likeartet og variasjonen gjelder særlig omfanget av regler. Utfordringen for brukerne av lovene og forskriftene er å se sammenhengene mellom regelverkene. På den måten unngår han at rettsreglene medfører at det utvikles flere isolerte strategier for å håndtere informasjonssikkerhet i en og samme virksomhet, for eksempel for internkontroll. I motsatt fall kan de *administrative byrdene* blir store for enkelte virksomheter. Dette har sammenheng med at reguleringene er kumulative og ikke valgfrie; jo flere regelverk som kommer til anvendelse på en og samme virksomhet, jo flere begreper skal forstås, roller bekles, risikovurderinger utføres, tilsyn gjennomføres, dokumentasjon fremlegges, pålegg etterleves, osv.

Se også vedlegg 3 (arbeidsgruppens anmerkning).

Skjønnsmessige målsettinger

Når det gjelder målsettingen for regelverkene, viser analysen at flere sikkerhetsbehov enn tidligere legges til grunn for regelverken. Hensynet til rikets sikkerhet og beredskap, som det dominerende sikkerhetsmålet, står for fall. Informasjonssikkerhet har flere formål og lover og regler om informasjonssikkerhet synes i hovedsak å forfekte dette mangfoldet. En vesentlig utfordring for lovgiver, regelverksforvalter og tilsyn ligger i å formidle budskapet om regelverkets tilpasning til virksomhetenes kontekst og reelle behov for sikring av informasjon. Det ligger en særlig utfordring i å tydeliggjøre hva som ligger i skjønsmessige begreper som *tilstrekkelig sikret*, *tilfredsstillende* eller *forholdsmessighet*. Dersom myndighetene ikke lykkes i dette arbeidet, er det nærliggende å tro at hensynet til samfunnets

funksjonsdyktighet og effektivitet - et hensyn som flere regelverk for øvrig legger til grunn - forspilles. I verste fall blir rettsreglene oppfattet som rigide og "stivbeinte", eller på andre måter tillegges negative betydninger. Dette er en nokså fundamental problemstilling som i verste fall kan undergrave sikkerhetsarbeidet. En følge kan bli at virksomheter unnlater å følge reglene (etterlevelsproblem) eller at myndighetene mister troverdighet som styrer av arbeidet med informasjonssikkerhet gjennom lover, forskrifter og instruksjoner (styrings- og legitimitetsproblem).

Mange tilsyn med tilnærmet likeartede oppgaver

Det er påvist et omfattende tilsynsregime som i større eller mindre grad har likeartede oppgaver som omhandler informasjonssikkerhet. Både private og offentlige virksomheter må forholde seg til flere tilsyn, direktorater og departementer samtidig. Fordi de enkelte lovene og forskriftene så å si har *sine egne tilsyn*, vil det være slik at jo flere lover og forskrifter en virksomhet må forholde seg til, jo flere tilsynsregimer og andre myndigheter skal ha et ord med i laget. Som nevnt mottar for eksempel fylkesmannen rettslige krav og forventninger om beredskapsplanlegging fra 11 departement og 8 direktorater (NOU 2000: 24, side 194). Det er ikke gjort systematiske analyser av hva *tilsynsregimet* faktisk pålegger virksomhetene, men det er grunn til å se nærmere på dette arbeidet i praksis.

Se også vedlegg 3 (arbeidsgruppens anmerkning).

Manglende hjemmel i forskriftene

Bestemmelser i enkelte forskrifter stiller krav som går lengre enn det strengt tatt finnes hjemmel for i lovgivningen. Spissformulert ser det ut til at praktiseringen og holdninger til bruk av lovhjemlene er utviklet noe tilfeldig. I enkelte situasjoner er det grunn til å se nærmere på om forskriftsprodusenten tar seg vel til rette og at det oppstår legalitetsproblemer. En slik analyse bør antakelig også inkludere andre kilder til informasjonssikkerhet enn forskriftene (rundskriv, instruksjoner, veiledninger, etc.). Hvis det er slik at forskriftene (eller for den sak skyld direktorater eller tilsyn) går lengre enn det som forutsettes av lovgiver, er det oppstått en (u)kultur som bør være gjenstand for nærmere vurderinger. Særlig bør lovgiver føre kontroll med at praktiseringen av de hjemlene som gis etterleves og ikke overdrives.

Det finnes også eksempler på at man i veiledninger bruk av uttrykk som *må* og *skal* der det skulle ha stått *bør* i henhold til regelen.

Se også punkt 4.4.6 (arbeidsgruppens anmerkning).

Avtaler og forhold til tredje part er ikke regulert

Undersøkelsen viser at de aller fleste regelverkene ikke omhandler avtaler og forhold til 3. part. Dette til tross for at mange virksomheter, både i privat og offentlig sektor, har satt bort hele eller deler av IT-tjenestene til eksterne firmaer. Det ligger antakelig en stor utfordring i å gjøre lover og forskrifter om informasjonssikkerhet gjeldende for eksterne leverandører.

Ikke enhetlig bruk av sanksjoner

Det er stor variasjon i bruken av sanksjonsformer (konsesjoner, bøter, erstatninger, straff, etc.). Derimot er det nokså like øvre strafferammer for lovbrudd. Fordi vi ikke har empiriske studier som viser effekten av ulike typer sanksjoneringer i arbeidet med informasjonssikkerhet, er det imidlertid vanskelig å si noe om effekten av sanksjoneringene på arbeidet med informasjonssikkerhet. Dessuten ble det antydnet (men ikke systematisk undersøkt) at sanksjoneringene i liten grad anvendes i praksis. En mulig konsekvens er at en del virksomheter velger å ignorere regelverkene fordi konsekvensene forbundet med lovbrudd er mindre enn kostnadene forbundet med etterlevelse av regelverkene.

Stor variasjon i detaljeringsgrad og gjenbruksteknikker

Et hovedfunn når det gjelder lovstruktur er at det er stor variasjon i detaljeringsgrad og gjenbruksteknikker. Om lag halvparten av regelverkene fremstiller informasjonssikkerhet overordnet (generelt), mens den andre halvparten regulerer informasjonssikkerhet nokså detaljert. Detaljerte regelverk skjer enten i form av nye regler eller gjenbruk av regler fra andre regelverk. Å henvise til standarder er nokså sjeldent. Et litt overraskende funn er at det ikke går noe klart skille i form av at lovene er generelle, mens forskriftene er detaljerte. Mange forskrifter er til dels svært generelle, og i noen tilfeller er lovene nokså detaljerte.

Gjennomgangen viser også at regelverkene er svært fragmentert og at den ikke følger noen klar logikk. Spissformulert kan vi si at valg av lovstruktur er tilsynelatende tilfeldig hva angår informasjonssikkerhet. Det er derfor grunn til å anta at brukeren må avsette mye tid til å finne ut hvilke regelverk som egentlig gjelder for sin virksomhet og hva som faktisk er gjeldende rett. I enkelte tilfeller må brukerne forholde seg til svært mange forskjellige kilder samtidig.

Ulike samordningsteknikker

Det finnes dessuten svært forskjellige teknikker for å samordne regelverkene (tematisk, virketid, opplysningstype, virkemidler, mv). Mest vanlig er det å samordne regler etter tema. Men også virketid og opplysningstyper anvendes. Kun ett regelverk omhandler informasjonssikkerhet eksplisitt og det er forskriften om informasjonssikkerhet til sikkerhetsloven. Denne forskriften er til gjengjeld nokså omfattende, med over 40 sider og om lag 200 hovedparagrafer. Konsekvensene av dette er at brukeren i hovedsak alltid vil finne reglene om informasjonssikkerhet i en *annen* kontekst enn *informasjonssikkerhet*. Det er usikkert om dette er en hensiktsmessig samordningsteknikk.

Ulik begreps- og språkbruk

Undersøkelsen viser at terminologi og språkbruk er svært problematisk i regelverkene om informasjonssikkerhet. Mange av begrepene er dessuten vage og ikke, eller dårlig, definerte. De fleste formuleringene er dessuten vanskelig å konkretisere i form av håndgripelige tiltak for å beskytte informasjon hos brukeren. At de i hovedsak heller ikke er spesielt godt koordinert, fører

antakelig i neste omgang til at reguleringen sett fra brukerens ståsted neppe oppleves som spesielt vellykket. Særlig når virksomheter må forholde seg til flere regelverk samtidig, noe som må sies å være hovedregelen og ikke unntaket.

Følgende forhold omkring språkbruken kan fremheves: Det er stor variasjon i hvordan begrepet *informasjonssikkerhet* anvendes og det forklares svært sjeldent i regelverkene. Heller ikke underkategorier som *konfidensialitet*, *integritet* og *tilgjengelighet* forklares. Suffikset *informasjon* er også uklart: Begrepene *datasikkerhet*, *meldingssikkerhet* og *dokumentetsikkerhet* er brukt. Vi ser i tillegg at det anvendes et svært stort omfang av andre begreper i lovene og reglene for å uttrykke mer eller mindre det samme fenomenet.

Det er videre identifisert ulike *5 typer sikkerhetsgraderinger* og det er usikkert om dette er en veloverveid strategi. Når det gjelder å forklare hvordan informasjon skal sikres i praksis, forsterkes inntrykket av en omfattende flora av vanskelige og fagspesifikke termer og sjargonger som antakelig kan assosieres til ulike departementer (såkalt "søylekultur"²²).

Det er manglende eller uklare formuleringer av *formål* og svært forskjellig plassering av selve bestemmelsene om informasjonssikkerhet.

Antakelig bidrar en ukoordinert språkbruk til at regelverkene om informasjonssikkerhet oppleves som vanskelig tilgjengelige for mange brukerne. Det blir kort sagt komplisert å konkretisere ord og uttrykk i form av håndgripelige og målbare tiltak for å beskytte informasjon. Særlig er dette en aktuell problemstilling for de mange private og offentlige virksomhetene som må forholde seg til flere regelverk samtidig. Isolert sett er kanskje eksemplene på termer og språkbruk den klareste indikasjonen på at regelverkene om informasjonssikkerhet ikke er tilfredsstillende koordinert mellom de ulike ansvarlige myndighetene. Rettspedagogisk er reglene om informasjonssikkerhet langt fra noe skoleeksempel.

Kommentardel til forskriften kunngjøres i Lovdata

Endelig er det i en del forskrifter anvendt til dels svært omfattende kommentarer som fremstår som en del av regelverket. Som eksempler kan nevnes internkontrollforskriften (HMS), forskrift om pasientjournal og flere andre forskrifter til helseregisterloven.

Ulike krav til virkemidler for å sikre etterlevelse

Det er nokså stor variasjon i reglene når det gjelder hvilke virkemidler som må tas i bruk av virksomhetene for å sikre etterleve regelverkene.

Tiltak som gjelder avklaring av ledelse og andre roller

Det klart mest populære tiltaket er å sørge for å avklare ledelse og andre roller. Et hovedfunn at det er det nokså forskjellige og uklare begreper og "merkelapper" som benyttes for å tildele roller og ansvarsforhold i

²² Sektorinndelingen kan se ut til å bidra til utvikling av sektorvise terminologier og begrepsforståelse.

regelverkene. Dette skaper i neste omgang potensielle rollekonflikter, uklare ansvarsforhold, osv. Isolert sett virker kanskje de enkelte rollene rasjonelle og klare. Det er innenfor de enkelte regelverkene etablert sentrale begrep som innbyrdes er tilsynelatende konsistente. Men når vi ser flere regelsett samlet, fremkommer det nokså mange *roller* og bildet blir uskarpt. Den store utfordringen for brukeren er å se disse rollene samlet. Ikke minst fordi de enkelte rollene ofte tilføres en lang rekke organisatoriske tiltak. Den store utfordringen for myndigheten er å legge forholdene til rette at det ikke pålegges unødige ”stillinger” for virksomhetene.

Det er et *svært* omfattende sett av oppgaver som følger av ansvaret for informasjonssikkerhet. Mange av regelverkene som er gjennomgåtte stiller konkrete og til dels svært omfattende krav til hvordan informasjonen skal sikres. Særlig er det kanskje grunn til å se nærmere på det om alle dokumentasjonskravene som fremmes er nødvendige, eventuelt. kan samordnes bedre. Dette gjelder også pålegg om internkontroll, utvikling av risikoanalyser, sikkerhetsstrategier, etc. Det er naturligvis også vesentlig at alle kravene er veloverveide og godt koordinerte på tvers av sektorene fra lovgiver eller forskriftsprodusentenes side.

Tiltak som gjelder opplæring og informasjon

Undersøkelsen viser også at om lag halvparten av regelverkene har bestemmelser om pedagogiske virkemidler. Når slike regler imidlertid finnes, er det særlig fire kategorier som går igjen: øvelser og opplæring av personell, krav til testing av tekniske løsninger og personell som skal betjene det tekniske utstyret, krav om fagkompetanse samt en del bestemmelser om informasjonsplikt, veiledningsplikt, mv. Kravene om øvelser etc., er særlig relatert til beredskapstenkning (krise og krig). En mulig konklusjon er at flere regelverk i større grad kan vektlegge de pedagogiske sidene ved sikkerhetsarbeidet. Men dette forutsetter en koordinert tilnærming slik at eventuelle tester, treninger og opplæringer ikke utvikles i isolasjon.

Tekniske tiltak

Et kanskje et litt overraskende funn er at det finnes få konkrete eksempler på at virksomheten pålegges å anvende teknologi for å beskytte informasjon. Det finnes noen unntak, men i hovedsak er disse teknologinøytrale og nokså vage. Illustrerende begreper som anvendes er krav om bruk av *tekniske hjelpemidler* eller *tekniske tiltak*. Det er usikkert om dette er en veloverveid regulatorisk metode.

Økonomiske tiltak

Endelig viser undersøkelsen at det er få bestemmelser som regulerer økonomiske sider ved sikkerhetsarbeidet. I de tilfellene vi finner er det særlig ulike former for refusjoner som er omhandlet. Det finnes imidlertid enkelte unntak i form av for eksempel krav til budsjettering. Likevel er det ingen tvil om at det er lagt nokså liten vekt på de økonomiske sidene ved sikkerhetsarbeidet i de gjennomgåtte regelverkene. Om dette er en hensiktsmessig strategi er et vanskelig spørsmål. Det er imidlertid liten tvil om at økonomi vil være en svært sentral faktor for å realisere informasjonssikkerhet. Særlig dersom virksomheten ”velger” å ta hensyn til alle

kravene som stilles i regelverken om informasjonssikkerhet, men dette vet vi som sagt lite om.

4.4.5 Om veiledninger til reglene og bruken av dem

Det er utarbeidet veiledningsmateriale til de mest sentrale regelverkene. Det er grunn til å tro at det som regel er veiledningene brukerne leser og forholder seg til. Hvordan disse formuleres, får derfor stor betydning for hvordan reglene etterlevs. Dette er blant annet omtalt av Torstein Eckhoff og Hans Petter Graver vedrørende plan- og bygningsregelverket.²³

Se Johs. Hansen Hammer: *Informasjonssikkerhet. Risikovurdering og sikkerhetsstyring – metoder og verktøy. En vurdering av egnethet for SMB*, kapittel 6 hvor han vurderer de enkelte veiledningenes egnethet for brukerne.

4.4.6 Manglende empiriske studier av rettsreglenes effekter

Med unntak av e-forvaltningsforskriften og IKT-forskriften er det ikke foretatt noen systematisk empiriske studier av den faktiske effekten av rettsreglene om informasjonssikkerhet. Heller ikke i forbindelse med Seip-utvalget²⁴ samordningsinitiativet²⁵ eller sårbarhetsutvalget²⁶ ble det gjennomført noen empiriske studier.

Allerede på slutten av 1970-tallet påpekte Wilhelmsen at vi vet for lite om *den fungerende retten*.²⁷ I mellomtiden har vi fått et betydelig mer omfattende regelverk og teknologi å forholde oss til. Fremdeles vet vi svært lite om disse reglenes faktiske effekt for forvaltningen, brukerne og samfunnet som helhet. For eksempel vet vi ikke hvor mange virksomheter som i det hele tatt anvender regelverkene, om de fungerer tilfredsstillende eller hva de koster næringslivet og samfunnet.

5 Anbefalinger

Vi starter dette kapitlet med å gjengi i sin helhet et notat fra medlem i arbeidsgruppen, professor dr. juris Dag Wiese Schartum, avdeling for forvaltningsinformatikk (AFIN), UiO. Her gir han kort en bakgrunn for temaet og et prinsipielt viktig forslag til tiltak. Hensikten er på en metodisk og helhetlig måte å ivareta både myndigheters og brukeres behov knyttet til regelverk og informasjonssikkerhet. Innholdet i notatet er presentert og diskutert i arbeidsgruppen, men notatet er fullt ut Schartums arbeid. Arbeidsgruppen mener dette er en høyst nødvendig helhetstenkning, som også har en prinsipiell interesse i forhold til regelverk generelt. Den tenkningen og

²³ Eckhoff, Torstein og Graver, Hans Petter, Plan- og bygningsloven og byggeforskriftene i praksis. Med kommentarer. Oslo: Tano 1992.

²⁴ NOU 1986:12 Datateknikk og samfunnets sårbarhet

²⁵ Samordning av regelverk for beskyttelse av informasjon. Rapport fra arbeidsgruppe (FD, JD, AAD) 1991

²⁶ NOU 2000:24 Et sårbart samfunn. utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet

²⁷ Jan Fredrik Wilhelmsen: Rettsregler om datasikkerhet, skriftserien jus og EDB nr. 23, 1977

det konkrete forslaget som Schartum her gjør seg til talsmann for, ønsker medlemmene i arbeidsgruppen å følge opp gjennom sitt praktiske arbeid i egenskap av ulike tilsyn og departement. Kapittel 5.1 med underpunktene 5.1.1 – 5.1.9 er skrevet av Schartum med tilhørende bruk av jeg-formen.

5.1 Notater om å ivareta informasjonssikkerhet ved hjelp av regelverk

5.1.1 Introduksjon

I dette notatet vil jeg presentere synspunkter på informasjonssikkerhet og regelverk som regulerer slik sikkerhet. Jeg vil dessuten skissere enkelte mulige arbeidsmåter som kan antas å være til nytte i det videre arbeidet med å forbedre informasjonssikkerhetsregelverket i Norge. Notatet referer ikke til andres arbeid, men prøver å se på spørsmål vedrørende regelverk for sikring av informasjon med "friske øyne". Samtidig er det imidlertid klart at deler av notatet er inspirert av resultater fra andres arbeid. Særlig gjelder dette arbeidet som forsker Are Vegard Haug ved Avdeling for forvaltningsinformatikk har utført vedrørende kartlegging og diskusjon av sikkerhetsregelverk.²⁸

I første avsnitt av notatet diskuterer jeg hva informasjonssikkerhet og informasjonssikkerhetsregelverk er. Dette er et spørsmål som mange muligens vil mene har opplagte svar, men som jeg antar bør drøftes for lettere å kunne identifisere de deler av informasjonssikkerhetsarbeidet som bør prioriteres. I avsnitt 5.1.3 skisserer jeg en modell for regelverksarbeid som etter min mening er anvendelig for arbeidet med sikkerhetsregelverk. Denne modellen forutsetter bruk av teknikker, verktøy og organisering som virkemidler i de ulike trinnene i arbeidet med regelverk. Regelverk som pålegger plikter eller innskrenker rettigheter og som dessuten er ressurskrevende å etterleve for "pliktsubjektene" vil lett skape motsetningsforhold. I avsnitt 5.1.4 gjør jeg en enkel beskrivelse av mulige hovedmotsetningsforhold i sikkerhetsarbeidet, og antyder noe om mulige implikasjoner for valg av reguleringsstrategi. I avsnitt 5.1.5 drøfter jeg med bakgrunn i slike eventuelle motsetninger, og mulige implikasjoner for utforming av regelverk som kan sikre mest mulig effektiv styring (avsnitt 5.1.5). Resten av notatet (avsnittene 5.1.6 – 5.1.8) inneholder skisser av slik virkemiddelbruk som jeg forutsetter i modellen for regelarbeidet i avsnitt 5.1.4. Stikkord her er teknikker for samordning av regelverk (avsnitt 5.1.6), verktøy for forarbeider, regelanvendelse og evaluering (avsnitt 5.1.7), og organisering av rettsanvendelsen (avsnitt 5.1.8). Avslutningsvis gir jeg noen råd om det videre arbeidet med informasjonssikkerhetsregelverk.

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

²⁸ Haugs arbeid var ultimo mai 2005 under ferdigstilling for publisering.

5.1.2 Allment om regelverk vedrørende informasjonssikkerhet

Informasjonssikkerhetsregelverk betegner – naturlig nok – regelverk som skal sikre informasjon. Noen ganger brukes også betegnelsene "datasikkerhet" og "datasikkerhetsregler". Ut i fra et vanlig skille mellom informasjon og data, kan det være naturlig å legge noe forskjellig mening i de to begrepene.²⁹ Til tross for en mulig meningsforskjell, velger jeg her å oppfatte datasikkerhet og informasjonssikkerhet som – i utgangspunktet – synonyme begreper. Imidlertid ser det ut til å være "informasjonssikkerhet" som er den dominerende betegnelsen for de relevante regelverkene som er vedtatt de siste 10 årene. "Informasjonssikkerhet" ser samtidig ut til å betegne regelverk som representerer helhetlige tilnærminger til informasjonssikkerhet. Med det mener jeg at ambisjonen er å ivareta de tre tradisjonelt viktigste sikkerhetsaspektene (konfidensialitet, integritet og tilgjengelighet), og at det anvendes mange tiltakstyper for å sikre informasjonen (organisatoriske, tekniske, fysiske osv). I de siste årene er "datasikkerhet" lite anvendt i regelverk, og har tidligere mest blitt brukt om enkeltstående bestemmelser, dvs bestemmelser som ikke uttrykker noen helhetlig tilnærming til informasjons-/datasikkerhetsområdet.³⁰

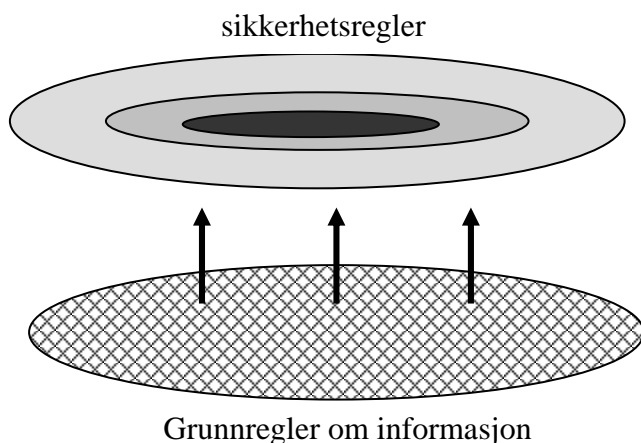
"Sikkerhet" og "sikring" kan selvsagt også gjelde annet enn informasjon. Sikkerhet kan for eksempel gjelde helse- og miljø, brann- og eksplosjon, trafikk/transport, el-forsyning osv. Selv om slike sikkerhetsspørsmål i utgangspunktet utgjør selvstendige områder, er det viktig å understreke at informasjonssikkerhet er innvevd i disse andre sikkerhetsområdene. Fordi informasjonssystemer styrer sentrale prosesser på nær sagt alle livsområder, vil det ofte være betydelige elementer informasjonssikkerhet i alle sikkerhetsområder. Et godt eksempel på dette er forskrift av 16.12.2002 nr 1606 om beredskap i kraftforsyningen, der informasjonssikkerhet er en integrert del av den samlede reguleringen, se kapittel 6 i forskriften.

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

²⁹ "Data" er noe som, når de blir fortolket, gir "informasjon" til brukeren. Informasjon er med andre ord det en kan utlede av data. Fordi data kan fortolkes innenfor mange referanserammer, kan det utledes forskjellig informasjon fra samme data.

³⁰ Se om dette i Dag Wiese Schartums artikkel "Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning", under publisering i Nordisk årbok i rettsinformatikk 2004, Norstedts forlag, 2005.

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



Figur 1: Samspillet mellom grunnregler og sikkerhetsregler

Personopplysningsforskriften, E-forvaltningsforskriften, IKT-forskriften og informasjonssikkerhetsforskriften er eksempler på slike regelverk. Denne typen regelverk angir samtidig tyngdepunktet i de seneste årenes regulering av informasjonssikkerhet.³¹

Midterste sone betegner sikkerhetsregler i form av mer enkeltstående bestemmelser, dvs bestemmelser som løser konkrete problemer, for eksempel som respons på en uheldig hendelse eller lignende.³² Begge disse kategoriene representerer eksplisitt regulering av informasjonssikkerhet, fordi kravet om sikring går direkte frem av rettsreglene. I ytterste sone av figuren finner vi imidlertid "implisitt" regulering av sikkerhet, dvs der det ikke sies i klartekst at sikkerhetstiltak skal treffes, men hvor dette følger indirekte av regler i lov eller forskrift eller av uskrevne rettslige prinsipper. Det viktigste eksempelet på siste kategori er grunnregler i kombinasjon med internkontrollbestemmelser, dvs bestemmelser som pålegger rettssubjektene å vurdere om det er behov for å iverksette tiltak for å sikre etterlevelse av rettsregler for øvrig. Kombinasjonen av internkontrollbestemmelser og grunnregler som stiller krav til konfidensialitet, integritet og tilgjengelighet, kan med andre ord ses på som sikkerhetsbestemmelser. På lignende måte kan for eksempel prinsippet om forsvarlig saksbehandling i kombinasjon med regler som gir krav på tilgang til informasjon, innebære en forpliktelse til å iverksette tiltak for å sikre slik tilgang. Etter offentlighetsloven bestemmer forvaltningsorganet innenfor

³¹ Se Dag Wiese Schartums artikkel "Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning", under publisering i Nordisk årbok i rettsinformatikk 2004, Norstedts forlag, 2005.

³² Se for eksempel forskrifter av 25.02.2000 nr 298 om Den norske kirkes medlemsregister, som i § 10 regulerer datakvalitet og tilgjengelighet, samt fastsetter regler om varsling av Datatilsynet i tilfellet av datainnbrudd.

rammene av krav til forsvarlig saksbehandling hvorledes gjennomføringen av innsyn skal skje. Dersom krav til forsvarlig saksbehandling tilsier det, må de med andre ord treffe tiltak som sikrer tilgjengeligheten.

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

Dersom vi ser på de grunnreglene om informasjon som bestemmelser om informasjonssikkerhet skal ivareta etterlevelsen av, er dette konvensjonelt krav vedrørende konfidensialitet, integritet og tilgjengelighet. En kan imidlertid tenke seg sikkerhetsregler som skal ivareta etterlevelsen av flere andre grunnregler; for eksempel regler om informasjonskvalitet, entydig identifisering av personer/virksomheter/objekter som det er knyttet informasjon til, autentisering av personer som gjør bruk av informasjonssystemer og annet. Hva som tas med når informasjonssikkerhet skal ivaretas, er dels et spørsmål om konvensjon, dels et spørsmål om hensiktsmessighet. I norsk regelverk finnes det eksempler på bestemmelser som går videre enn det som er vanlig for informasjonssikkerhet. I helseregisterloven er det for eksempel tatt inn en bestemmelse i § 16 om " Sikring av konfidensialitet, integritet, *kvalitet* og tilgjengelighet" (min kursiv).³³ En helhetlig tilnærming til informasjonsbehandling kan tilsi at dette er en hensiktsmessig løsning. Dersom en imidlertid ser på hva slags kompetanse som kreves for å ivareta de ulike elementene i kravene til sikring, kan det være en kommer til motsatt resultat. Sikring av konfidensialitet, integritet og tilgjengelighet er i stor grad noe som kan sikres gjennom fysiske, tekniske og teknologiske tiltak, og i tillegg "organisatoriske" tiltak vedrørende systemarkitektur, konfigurering av systemet mv. Slike spørsmål kan håndteres av "teknologer", og disse spørsmålene oppstår i tilknytning til ethvert informasjonssystem. Derfor er dette "globale" informasjonssikkerhetsspørsmål.

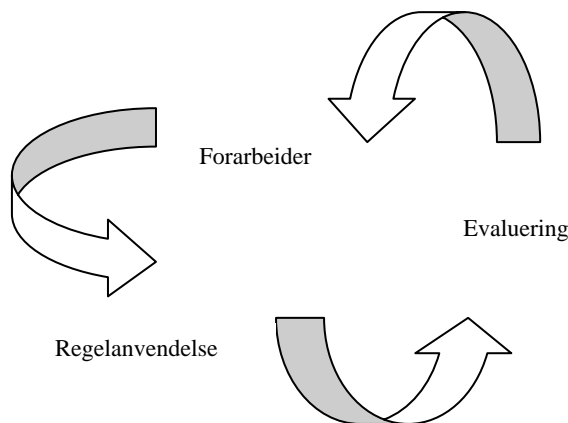
Når det gjelder kravene til opplysningskvalitet, trenger en ofte en helt annen type kompetanse. For å vurdere om opplysninger er relevante, fullstendige og korrekte mv, må vurderingen skje innen spesifikke faglige rammer og i forhold til bruksformålet. Opplysningskvalitet i helsesektoren er med andre ord et medisinskfaglig spørsmål, i offentlig forvaltning er det ofte et forvaltningsrettslig spørsmål, og innen anleggsbransjen er det kanskje et

³³ Et annet eksempel er forskrift om Den norske kirkes medlemsregister, se forrige fotnote.

ingeniørfaglig spørsmål. Slike sikkerhetsspørsmål er ikke "globale" men fagspesifikke; dvs de er relevante for informasjonssystemer innen et visst fagområde. Her tar jeg ikke stilling til hvilken systematikk som er mest hensiktsmessig. Poenget er bare å understreke at avgrensingen og kategoriseringen av spørsmål vedrørende informasjonssikkerhet ikke er "naturgitt", men er bl.a. avhengig av en rekke pragmatiske vurderinger.

5.1.3 Helhetlig blikk på regelverksarbeid

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



Figur 2: "Regelverkssyklus"

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

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

- organisering,
- metodikk og
- verktøy.

Sett i sammenheng med det som er sagt ovenfor, betyr de nevnte virkemiddeltypene at målet må være å sette inn slike virkemidler som er egnet til å tilrettelegge for neste stadium av arbeidet. Spørsmålet blir dermed (bl.a.) hvilke organisatoriske tiltak under forarbeidene er egnet til å lette

regelanvendelsen? Hvilke metodikker under regelanvendelsen er egnet til å lette evalueringen? [osv] I dette notatet har jeg bare anledning til å redegjøre for enkelte aktuelle virkemidler. Nedenfor vil jeg derfor si noe om mulige samordningsmetoder knyttet til forarbeidet (avsnitt 5.1.6), elementer av verktøy fordelt på alle tre trinn i syklusen (avsnitt 5.1.7), og til slutt litt om organisering av regelanvendelsen (avsnitt 5.1.8).

5.1.4 Motsatte perspektiver på regelstyring av informasjonssikkerhet

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

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

Et viktig perspektiv på arbeidet med informasjonssikkerhetsregelverk er som nevnt styrings- eller myndighetsperspektivet. Da ser vi spørsmålet om informasjonssikkerhetsregelverk som et spørsmål om hensiktsmessig politisk og rettslig styring, for å nå mål som er fastlagt gjennom det demokratiske styringssystemet. I dette perspektivet er det nærliggende å legge vekt på hva som representerer den mest effektive styringen. Det kan da være at rettsregler om informasjonssikkerhet kan gi effektiv styring alene. En annen mulighet er at regelverk kun gir effektiv styring under visse forutsetninger, og for eksempel i kombinasjon med andre styringsmidler (økonomiske, organisatoriske, pedagogiske mv). I dette perspektivet står det derfor helt sentralt å vurdere hva

som – samlet sett – gir den beste styringen mot de fastsatte politiske målene, og regelverk om informasjonssikkerhet kan være ett element. Når en eventuelt velger regelstyring, blir neste spørsmål hvilke krav som må stilles til denne for å oppnå best mulig virkning.

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

Selv om det i en viss grad må antas å være sammenfallende interesser mellom myndighets- og virksomhetsperspektivet, er det etter min mening grunn til også å forutsette at det ofte vil foreligge noen grad av motsetning. Det betyr at myndigheter som ønsker å bedre informasjonssikkerheten ved å gi regelverk, må legge vekt på å identifisere mulige mål- og virkemiddelkonflikter. Slik kunnskap bør brukes for om mulig å *harmonisere* ved å minske selve motsetningsforholdet. Motsetningsforholdet kan trolig reduseres ved å foreslå reguleringer som:

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

Oppfyllelse av kravene i 1) – 3) vil lett innebære at styringsambisjonene må reduseres. I et brukerperspektiv kan oppfyllelse av 4) på den andre siden tenkes å kompensere for manglende oppfyllelse av kravene i 1) – 3). Et omfattende regelverk som det er krevende å fortolke/forstå, kan for eksempel bli mer akseptabelt dersom det følger verktøy med som automatiserer og på annen måte legger til rette for så enkel anvendelse av regelverket som mulig, se avsnitt 5.1.7. Ut i fra denne enkle betraktningen kan det derfor antas at kraftige verktøy som gjør det lettest mulig å anvende regelverket, er en av nøklene til å redusere det antatte motsetningsforholdet mellom styringsperspektivet og virksomhetsperspektivet. Gitt et komplekst og vanskelig sikkerhetsregelverk (jf 1 – 3), kan verktøy bli avgjørende for regelverkets effektivitet, dvs for i hvilken grad styringsambisjonen vil bli realisert.

Selv om motsetningsforholdet mellom de to perspektivene eksisterer fordi motsetningsforholdet ikke kan harmoniseres (jf punktene 1 – 4), kan

betydningen av dette motsetningsforholdet reduseres. Således kan myndighetene for eksempel tvinge igjennom etterlevelse ved hjelp av kontroller og sanksjoner. En annen mulighet er å bruke positive tiltak, for eksempel ved å gi økonomisk kompensasjon for ressursbruk. Selv om motsetningsforholdet kan reduseres, antar jeg at en slik strategi neppe er særlig aktuell som hovedstrategi, og at en viss grad av harmonisering derfor som oftest vil være et ønskelig element.

5.1.5 Kommunikasjon av sikkerhetsregelverk

Utgangspunktet for den følgende diskusjonen er at sikkerhetsregler er uttrykk for ønsket om effektivt å styre sikkerhetskritisk informasjonsbehandling, jf styringsperspektivet i forrige avsnitt. Denne styringen kan være politisk og/eller faglig begrunnet. Her går jeg ikke nærmere inn på spørsmål vedrørende det materielle innholdet av sikkerhetsreglene og de mulige motivene for vedtakelse av regler. Utgangspunktet er kun at det foreligger en legitim ambisjon om å styre informasjonssikkerhet, og at utforming av regelverk er en betydningsfull del av denne styringen. Spørsmålet blir da hvorledes slike sikkerhetsregler bør utformes for å sikre mest mulig effektiv styring. Det er neppe grunn til å tro at det finnes allmenngyldige svar på et slikt spørsmål, og siktemålet her er derfor kun å peke på relevante "tankeskjemaer", hensyn og tiltak som kan være til hjelp i bestrebelsene for å etablere en effektiv regelstyring. Den følgende diskusjonen kan ses som en ekspansjon og videreutvikling av den enkle listen (med punktene 1 – 4) i forrige avsnitt.

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

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

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

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

rettslige, økonomiske, pedagogiske og eventuelt andre aspekter ved reguleringen.

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

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

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

Før det skjer en tilpasning, er det grunn til å se nærmere på enkelte forhold som må antas å ha betydning for hvor lett eller vanskelig det vil være å kommunisere innholdet av et regelverk, jf i) ovenfor. Den følgende gjennomgangen er ikke ment å være fullstendig, men antas å omfatte flere forhold som ofte kan være av vesentlige betydning. Jeg kommer ikke her nærmere inn på forhold knyttet til iverksettelsen av regelverk i den enkelte virksomhet, jf ii) ovenfor. Dette vil imidlertid bli nærmere belyst i AFINs prosjekt "Legal Information Security Regulations - An instrumental perspective", som vil bli gjennomført i perioden høsten 2005 – høsten 2007.³⁴

Sikkerhetsreglene inngår i "egne" regelverk

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

³⁴ Prosjektet er finansiert av forskningsprogrammet IKT-SoS ved Norges forskningsråd.

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

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

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

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

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

Regelverket har fellestrekk med kjente reguleringer

Det er også grunn til å tro at regelinhold best kan kommuniseres dersom det kan inngå som en integrert del av elementer i et eksisterende regelverk, og således bygger på noe den enkelte "regelverkbruker" allerede er kjent med. Dette gjelder særlig dersom "grunnregler om informasjon" og sikkerhetsbestemmelsen kan plasseres i sammenheng, jf avsnitt 5.1.2. Tanken er med andre ord at dersom en har et regelverk med bestemmelser om

taushetsplikt eller lignende, er muligheten best for vellykket kommunikasjon av relevante sikringsregler, dersom disse knyttes til taushetspliktbestemmelsen. I dette ligger det en antagelse om at "jo nærmere og mer integrert, jo større er muligheten for vellykket kommunikasjon. Dersom loven har en regel om taushetsplikt, vil det da være bedre å sette sikringsbestemmelsen direkte inn i sammenheng med denne bestemmelsen, enn å plassere den i en tilhørende forskrift eller i en annen del av samme lov.

Krever forhåndskunnskaper som adressatene har

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

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

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

Reglene er beskrevet som en arbeidsprosedyre

Det å forstå en regeltekst innebærer å skjønne hvorledes regelmyndigheten ønsker at vi skal forholde oss, fordi etterlevelse av rettsregler innebærer at vi må utføre noen handlinger. Problemet med å omsette ord til handling, handler bl.a. om å forstå hva som er "prosedyren". Regelverk er ofte fragmentarisk ved at det er formulert regelfragmenter som den enkelte regelanvender selv må sette sammen for å forstå hvorledes han skal forholde seg. Anvendelse av et fragmentert regelverk krever imidlertid generell problemforståelse og en viss juridisk kompetanse som en ikke uten videre kan forvente at den enkelte som skal etterleve sikkerhetsbestemmelsene har. Det kan derfor være grunn til eksplisitt å angi en prosedyre, dvs den konkrete fremgangsmåten som må følges for å nå et tilfredsstillende resultat: For den som kan lage sukkerbrød, er det nok

å få oppgitt hva ingrediensene skal være og vedkommende vil vite at det må følges en helt spesiell fremgangsmåte for å få et vellykket resultat. Uten denne kunnskapen, er det gode muligheter for et mislykket resultat selv om alle ingredienser er kjent med nøyaktige mål. På lignende måte kan en det være vanskelig å etterleve et sikkerhetsregelverk selv om alle "ingredienser" er kjent, dersom regelverket ikke samtidig er klart vedrørende rekkefølgen på utførelse av de ulike arbeidsstegene som loven gir anvisning på.

Vektlegging av arbeidsprosedyre innebærer en antagelse om at det er størst mulighet for vellykket kommunikasjon av sikkerhetsregelverk, dersom dette legger vekt på tydelige angivelser av tid/rekkefølge og relasjonene mellom de ulike regelementene. Dette innebærer at særlig at rekkefølgen av rettsreglene i størst mulig grad bør følge rekkefølgen ved en typisk utførelse/etterlevelse, og at det uansett er tydelige henvisningsstrukturer mellom de ulike regelementene. Sagt på en annen måte, speiler dette en antagelse om at regelverk der en tydeliggjør hvorledes den praktiske etterlevelsen skal skje, vil være lettere å kommunisere enn regelverk der en primært baserer seg på den enkeltes generelle bakgrunnskunnskaper og kompetanse i å anvende rettsregler. Dermed er det imidlertid ikke sagt at det alltid er mulig eller ønskelig å angi hvert steg knyttet til etterlevelsen. Igjen er dette avhengig av en totalvurdering, og hensynet til fleksibilitet kan for eksempel tilsi at en er tilbakeholdende med å angi bestemte prosedyrer som skal følges.

5.1.6 Samordning av sikkerhetsregelverk

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

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

Det kan også være ulemper knyttet til samordning. Dette gjelder særlig faren for manglende fleksibilitet i den politiske/faglige styringen ved hjelp av regelverket. Dersom behov for regelendring er begrunnet i behov knyttet til ett virksomhetsområde, mens det innen andre virksomhetsområder ikke eksisterer tilsvarende behov, kan en stå overfor valget mellom å bryte ut av samordningstilnærmingen, gi regler som har uønskede konsekvenser eller å la være å gi regler og tåle følgene av slik passivitet. Sikkerhetsforskriftene til SIS-loven er f.eks. nesten identisk med sikkerhetsbestemmelsene i

personopplysningsforskriften kapittel 2. Det er rimelig å tro at denne likheten kan være et argument i seg selv, og at det kan føre til at terskelen mot å endre SIS-bestemmelsene blir høyere, eventuelt at en er forsiktig med å endre personopplysningsforskriften fordi dette vil kunne igangsette parallelle forskriftsarbeider også på andre felt.

Jeg skal ikke her gå nærmere inn på en argumentasjon for eller i mot samordning av sikkerhetsregelverk. Før en slik vurdering kan skje, er det uansett grunn til å undersøke noe nærmere hva "samordning" kan tenkes å innebære. Nærmere analyse viser at begrepet samordning ikke gir noen klare svar i seg selv, og at det er en rekke mulige samordningstiltak å velge mellom. I det følgende vil jeg kort gjennomgå noen hovedalternativer. Alternativene er hentet fra min artikkel "Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning".³⁵ I artikkelen blir mulige samordningsteknikker identifisert og supplert med utgangspunkt i det sentrale norske sikkerhetsregelverket.

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

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

³⁵ Artikkelen er under publisering i Nordisk Årbok i rettsinformatikk, Norstedts forlag, 2005.

Mønsterregler. "Mønsterregler" betegner en strategi der det utarbeides et regelsett som en antar er gagnlige for mange virksomhetsområder, men der en i utgangspunktet aksepterer og har forventning om at det vil være behov for tilpasninger til de ulike elementene i regelverket. Resultatet blir i så fall regelverk som er like på noen områder, har felles trekk på andre områder og er ulike på atter andre områder. Ulempen med en slik tilnærming er at samordningseffekten kan komme til å bli liten dersom behovet er stort for å gjøre endringer i de mønsterreglene som danner utgangspunktet. Fordelen er selvsagt at en slik tilnærming gir en stor grad av fleksibilitet, samtidig som en viss grad av koordinering sikres.

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

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

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

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

forskjellige kriterier hadde vært anvendt. Dersom samordningseffekten skal bli merkbar, vil dette imidlertid trolig kreve ytterligere tiltak, for eksempel bruk av felles verktøy eller lignende, jf nedenfor i avsnitt 5.1.7.

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

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

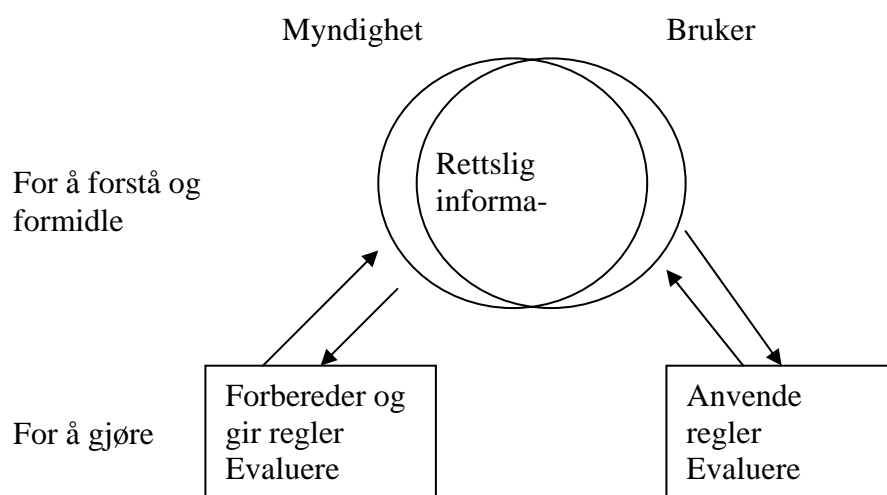
I tillegg til de 9 tilnærmingene til bedre samordning av informasjonssikkerhetsregelverk som jeg har nevnt ovenfor, er det flere mulig supplerende strategier som kan lede til bedre sammenheng mellom slike regler. Dette er med andre ord ikke fremgangsmåter som direkte gjelder utformingen av regelteksten,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

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

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

Innledning

"Verktøy" betegner her IKT-baserte hjelpemidler av ulike slag. Betegnelsen er upresis men populær, og har etter min mening den fordel at den erfaringsmessig gir en del viktige og riktige assosiasjoner. I figur 3 har jeg forsøkt å illustrere noen aspekter ved verktøybegrepet slik jeg her bruker det. Ideen er at det grunnleggende verktøyet er et rettslig informasjonssystem, dvs et system som



Figur 3: Grunnleggende struktur for mulige verktøy knyttet til

primært inneholder det relevante regelverket. Et slikt system bør trolig – stort sett - være likt for regelmyndigheter og brukere av sikkerhetsreglene, men i figuren har jeg antydnet at systemet kan tenkes å eksistere i versjoner for å ivareta særlige behov hos de to aktørene. De firkantede boksene indikerer verktøy som er utformet for å hjelpe myndigheter til å administrere regelverket (venstre boks), og for å hjelpe brukere til å utføre de oppgaver som sikkerhetsregelverket gir anvisning på (høyre boks). I boksene er det indikert hva henholdsvis myndigheter og brukere må gjøre, og disse oppgavene tilsvarer de tre stadiene i "regelverkssyklusen" som er beskrevet i avsnitt 5.1.3.³⁶ Pilene indikerer at prosessene går begge veier: Myndigheter både forbereder/gir reglene i informasjonssystemet og evaluerer dem, brukere både anvender og evaluerer regler. Brukernes evalueringer/tilbakemeldinger på grunnlag av regelanvendelsen, inngår i myndighetenes evaluering.

Verktøy kan tenkes å bidra til at samordningsmuligheter faktisk blir utnyttet når dette anses å være hensiktsmessig. Verktøyet for myndigheter kan for eksempel inneholde og legge til rette for bruk av bestemte regelverksarkitekturer, legaldefinisjoner, regelbibliotek mv. De kan også legge til rette for tilgang til og analyser av eksisterende regelverk, for eksempel basert

³⁶ I figur 3 har jeg likevel valgt å tydeliggjøre brukernes deltakelse i evalueringen av regelverk.

på en kategorisering av alle relevante regelverk vedrørende informasjonssikkerhet i henhold til regeltype, forekomster av begreper mv. Slik kan et verktøy legge til rette for å identifisere alle bestemmelser som vedrører sikkerhetsrevisjon eller avvikshåndtering osv. Det er etter min mening grunn til å tro at verktøy ofte vil være en forutsetning for å oppnå reelle samordningsresultater. Årsaken er at samordning ofte er så komplekst og arbeidsintensivt at praktisk tilrettelegging og forsiktig automatisering av støttefunksjoner mv vil være en forutsetning for at det skal skje en tilstrekkelig innsats. Hjelpemidlene kan også gjelde selve regelanvendelsen eller vurderingen av regelverk med tanke på endring og forbedring.

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

Verktøy for utarbeiding av sikkerhetsregelverk

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

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

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

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

I de aktuelle regelverkene bør en også innarbeide alle eksplisitte henvisningsstrukturer slik at det er lett å studere den sammenheng hvert regelverk/hver enkeltregel står i. Dette gjelder for det første internt i et informasjonssikkerhetsregelverk, og for det andre mellom ulike regelverk. I tillegg kan det være ønskelig å tydeliggjøre henvisning til "grunnreglene" så langt som mulig, dvs til de regler som fastsetter de adferdsregler mv som skal sikres. Når SIS-forskriften § 7-11 fastsetter plikt til å sikre konfidensialitet, bør

denne bestemmelsen således knyttes opp til alle bestemmelser på området som pålegger konfidensialitet (f.eks. SIS-lovens §§ 12, 13, 14 og 15, samt forskriftens § 7-9).

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

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

Et verktøy til bruk ved utarbeiding av sikkerhetsregelverk bør for det tredje gjøre tilgjengelig erfaringsmateriale vedrørende det regelverk som skal erstattes eller revideres, dvs materiale som utarbeides i samband med evaluering av tidligere regelverk. Se om dette, nedenfor i avsnitt 5.1.7.4.

Verktøy ved anvendelse av sikkerhetsregelverk

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

Et tekstrettet verktøy bør inneholde en kommentarstruktur, dvs en samling kommentarer som er knyttet til tekstelementer i regelverket på ulike nivåer.³⁷ Kommentarene skal sette den enkelte bruker i stand til å lese og forstå de aktuelle rettsreglene. Dette innebærer at det for det første bør være kommentarer som er begrunnet i regelmyndighetens behov for å forklare og presisere. Dersom regelverket er en lovtekst, vil de spesielle motivene i odelstingsproposisjonen kunne fungere som kommentarstruktur, eventuelt i redigert og supplert form. For det andre bør det være kommentarer som er utformet ut i fra de spørsmål som har kommet inn fra brukere vedrørende hvorledes regelverket skal forstås, jf neste avsnitt om evaluering. Denne siste delen av kommentarstrukturen skal med andre ord bygges gradvis opp gjennom bruk av verktøyet.

I tillegg til kommentarstrukturen bør det vurderes en parallell *eksempel*struktur, dvs det bør være eksempler knyttet til utvalgte deler av regelverket der dette

³⁷ Dvs til regelverket som sådan, til kapitler, enkeltbestemmelser, deler av en bestemmelse mv.

anses å være nødvendig eller nyttig for å illustrere konkrete anvendelser av bestemmelser. Eksemplene kan gjerne følge samme mønster som kommentarstrukturen og eventuelt være en integrert del av denne. Det betyr blant annet at enkelte eksemplifiseringer kan gjøres i utgangspunktet, mens supplerende eksempler kan gis som respons på spørsmål som oppstår i tilknytning til bruk av regelverket. Et tredje element kan være å gjøre tilgjengelig autoritative avgjørelser vedrørende fortolkning av bestemmelser i regelverket. Særlig er domsavgjørrelser og avgjørelser i klagesaker aktuelle.

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

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

Verktøy ved evaluering av sikkerhetsregelverk

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

En del av den tidligere omtalte kommentarstrukturen (jf avsnitt 5.17.3) ble knyttet til spørsmål som fremkommer under bruk av regelverket. Dette forutsetter for det første en funksjon som tillater brukere å formulere og sende inn spørsmål vedrørende fortolkning av bestemmelser. Det er for det andre en forutsetning at det er en myndighet som kan ha et løpende ansvar for å motta, vurdere og svare på innkomne spørsmål. Tanken er at enkelte spørsmål kan danne grunnlag for en forklarende kommentar, eventuelt med et eksempel (jf ovenfor). Andre spørsmål vil ikke bli besvart direkte i form av en kommentar, men inngå i et materiale som anvendes som grunnlag for periodisk evaluering

av regelverket. Også de spørsmål som resulterer i løpende kommentarer vil selvsagt inngå som grunnlag for evalueringen.

Avsluttende bemerkninger om verktøy

Ideelt sett utgjør de tre verktøy som ovenfor er skissert ett integrert hjelpemiddel som dekker hele regelverkets "livssyklus", dvs som kan gi støtte ved utarbeiding av reglene, bruk, evaluering, regelendring, bruk osv. Dette igjen betegner et regelverksarbeid som er basert på en kontinuerlig innsats for på den måten hele tiden å sikre så god kommunikasjon av regelinnhold som mulig, og samtidig stadig gjøre regelendringer som forbedrer kommunikasjon av regelinnhold og som derfor høyner måloppnåelsen, jf avsnitt 5.1.3.

5.1.8 Organisering av rettsanvendelse

Den siste skissen av virkemiddelbruk på de ulike trinnene i regelverkssyklusen (jf avsnitt 5.1.3), gjelder organisering av rettsanvendelsen. Poenget er da at organiseringen av rettsanvendelsen skal tilrettelegge for det neste trinnet, dvs for evalueringen av regelverket. Organisering av rettsanvendelsen ellers vil primært være et spørsmål om å organisere saksbehandlingsarbeidet hos det forvaltningsorganet som har kompetanse på vedkommende fagområde på en måte som gir effektiv ressursbruk, rettsriktige resultater og forsvarlig skjønnsutøvelse. Slike hensyn er åpenbart viktige og legitime, men er knyttet til enkeltsaksbehandlingen. Organisering av rettsanvendelse og saksbehandling kan imidlertid også skje ut i fra hensynet til evalueringen av regelverket, og slike hensyn kan også være gagnlig i forhold til enkeltsaksbehandlingen.

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

Et annet synspunkt er at innsamling av erfarings- og kunnskapsmateriale i tilknytning til rettsanvendelsen ikke bør begrenses til forvaltningens saksbehandlere. Ikke minst når det gjelder informasjonssikkerhetsregelverk er rettsanvendere utenfor forvaltningen av stor betydning. Særlig gjelder dette de som i henhold til regelverket skal etterleve bestemmelsene. Rettsanvendelsen bør derfor kunne organiseres slik at den legger til rette for å samle inn materiale fra flere grupper rettsanvendere (saksbehandlere, pliktige personer mv) over hele perioden for rettsanvendelse, dvs fra regelverket trådte i kraft til evalueringsfasen er innledet, jf figur 2 (ovenfor). Et verktøy som det jeg har skissert i avsnitt 5.1.7 (*Verktøy ved anvendelse av sikkerhetsregelverk*) kan ha slike organiserende effekter; Dvs verktøyet blir gjort attraktivt for flest mulige brukere av regelverket, og det legges til rette for fortløpende svar på tolkningsspørsmål mv (noe som kan motivere og øke bruken). Når en når frem til selve evalueringsfasen vil det foreligge et rikt "historisk" materiale. Dette kan suppleres i form av et retrospektivt materiale, dvs materiale som

fremkommer ved at en undersøger tidligere saksforhold og begivenheter og spør om hva involverte personer har av hukommelse og oppfatninger.

5.1.9 Avsluttende bemerkninger

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

Jeg tenker meg et opplegg der en gruppe bestående av personer fra regelmyndigheter og academia spesifiserer krav til et verktøy, dvs krav til et IKT-basert hjelpemiddel for bruk ved håndtering av sikkerhetsregelverk. Et slikt verktøy bør inneholde noen elementer på alle trinn i "regelverkssyklusen" (jf avsnitt 5.1.3), og særlig er det grunn til å dekke evalueringstrinnet.

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

5.2 Empiri og samordning

Dette kapittelet er skrevet av medlem av arbeidsgruppen, stipendiat Are Vegard Haug, Avdeling for forvaltningsinformatikk (AFIN), UiO. Teksten er hentet fra hans før omtalte studie.³⁸ I pkt 5.2.1 er teksten mildt bearbeidet fra "jeg-formen" til tredjeperson, uten å endre innholdet. I pkt. 5.2.2 er Haugs tekst gjengitt direkte. I pkt 5.2.3 er teksten sterkt forkortet og tilbake i tredjeperson.

5.2.1 Noen hovedfunn, som bakgrunn for forslag

Ut i fra målsettingen i den nasjonale strategien for informasjonssikkerhet (eNorge 2003), faglitteraturen om informasjonssikkerhet, kritikken i utredningene, omfanget av lover og forskrifter, med mer, har det utkrystallisert seg en del felles antagelser eller hypoteser om lovgivningen.

I hypotese 1 antok Haug at *antallet lover og forskrifter om informasjonssikkerhet har økt i antall og volum til tross for omfattende forsøk på regelverksforenklinger og saneringer*. Haugs gjennomgang styrket denne hypotesen. Det er påvist et nokså omfattende regelverk som omhandler informasjonssikkerhet, og det er en nokså dramatisk vekst i antall regelverk (særlig etter 1995-96). Om denne veksten vil fortsette er mer usikkert.

³⁸ **Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet?** Arbeidet er i skrivende stund (slutten av mai 2005) under ferdigstilling for publisering.

I hypotese 2 antok Haug at *lovene og forskriftene om informasjonssikkerhet i liten grad er koordinert. Og at det finnes flere eksempler på overlapping som gjør at virksomhetene må forholde seg til flere regelsett om informasjonssikkerhet samtidig.* Også denne hypotesen er styrket. Flere av eksemplene i (kapittel 6) (HVOR I VÅR RAPPORT?) peker i denne retningen. I ekstreme situasjoner fant Haug at noen virksomheter må forholde seg til over 10 regelverk samtidig.

I hypotese 3, antok Haug at *fordi reguleringene ikke er godt koordinert skaper de unødige problemer og kostnader for virksomhetene.* Denne hypotesen er også styrket, men dataene som er samlet inn er ikke tilstrekkelig for å teste hypotesen. Til det trenges det empiriske studier av hvilken effekt rettsreglene egentlig har på virksomheter.

Med disse overordnede funnene for øyet hevder Haug at det kanskje særlig er to grep som skal til for å forbedre arbeidet med de rettslige reguleringene av informasjonssikkerhet.

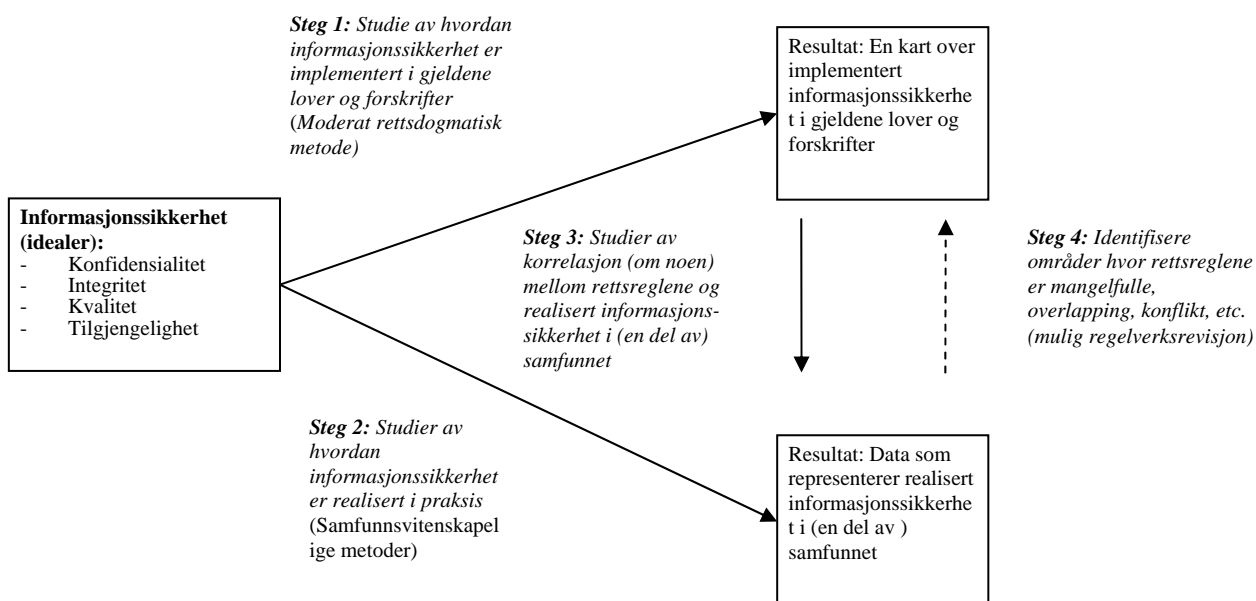
5.2.2 Behovet for et bedre og empirisk basert beslutningsgrunnlag for videreutvikling av regelverkene om informasjonssikkerhet

For det første må det fremskaffes et *bedre empirisk basert beslutningsgrunnlag for det videre arbeidet.* Hovedutfordringen ligger i å utvikle et forskningsteoretisk utgangspunkt for en empirisk drevet videreutvikling av regelverkene om informasjonssikkerhet. Deretter bør det gjennomføres tester av effekten av reglene på et utvalg relevante virksomheter. Kanskje kan den instrumentelle virkemiddelmodellen som er presentert i kapittel 4 (i Haugs utredning, ikke denne, red.anm.) anvendes som et utgangspunkt, men ytterligere operasjonaliseringer er nødvendige. I dette resonnementet ligger det en anerkjennelse av det faktum at det nærmest er fullstendig mangel på empiriske anlagt forskning omkring den faktiske effekten av de regulatoriske strategiene som er valgt for å regulere informasjonssikkerhet. Normative studier, herunder de mange studiene av rettslige reguleringer av informasjonssikkerhet (Wilhelmsen 1977, NOU 1986:12, Samordningsutvalget 1991, Sårbarhetsutvalget 2000, m.fl.), har i all hovedsak vært opptatt og styrt av rettsdogmatiske modeller og tanke sett. Spørsmål om kausalitet mellom de forskjellige virkemidlene som lovgiver velger (bevisst eller ubevisst) og realisert informasjonssikkerhet i samfunnet er i hovedsak ubesvart. Poenget er at det gjennom instrumentelle modeller synes mulig å koble disse to tradisjonene (normativ og empirisk forskning) sterkere sammen. Uten en empirisk anlagt forskning er det svært vanskelig, for ikke å si umulig, å vite i hvilken grad lovgivers intensjoner med lovgivningen virkelig blir realisert.

Forutsetning for bruk av modellen er som tidligere nevnt at det stilles til disposisjon flere typer viten: Empirisk-teoretisk kunnskap om sammenhengene i en slik modell, normativ- teoretisk kunnskap om verdspørsmålene, og metodisk kunnskap som gjør det mulig å diagnostisere adferd og holdninger. Fordi de forskjellige profesjonene og fagtradisjonene sjelden alene dekker alle disse kunnskapene, kreves det både anerkjennelse for samarbeid og faktisk samarbeid. Konkret kan en slik forskningsstrategi konsentreres omkring følgende overordnede analysemodell fordelt på fire steg, jf modell 10.

Steg 1 er studier av hvordan informasjonssikkerhet er implementert i gjeldende lover og forskrifter. Denne delen av studien forutsetter en moderat rettsdogmatisk metode, og kanskje kan denne rapporten (Haug's rapport, red. anm.) anvendes som utgangspunkt for dette arbeidet. Resultat fra analysen er et kart over implementert informasjonssikkerhet i gjeldende lover og forskrifter.

Figur 1) Overordnet analysemodell for det videre arbeidet med rettslige reguleringer av informasjonssikkerhet:



I steg 2 av studien er hovedutfordringen å kartlegge hvordan informasjonssikkerhet er realisert i praksis. Dette krever en eller annen form for samfunnsvitenskapelig metode. Som vist over er det behov for ytterligere operasjonaliseringer, med påfølgende innsamling av empiri. Resultatet fra undersøkelsen vil gi viktige data som representerer realisert informasjonssikkerhet i (en del av) samfunnet. Det bør også samles inn eller gjenbrukes bakgrunnsdata om virksomhetene som kan anvendes for å forklare variasjon gjennom for eksempel statistiske hypotesetestinger (størrelse, organisasjonstyper, ledelse, økonomi, teknologibruk, etc.).

Steg 3 går ut på å studere korrelasjon (om noen) mellom rettsreglene og realisert informasjonssikkerhet i (en del av) samfunnet. Dette kan for eksempel skje gjennom multivariate analyser og bruk av statistiske data. Men også andre metoder er hensiktsmessige. For eksempel vil det være mulig å kartlegge hvilke rettsregler (om noen) som er lagt til grunn for arbeidet med informasjonssikkerhet, erfaringer med disse, betydninger av spesifikke typer tiltak, osv.

I steg 4 vil det være mulig å identifisere områder hvor rettsreglene oppleves som mangelfulle, overlappende, konflikter, etc. basert på data fremskaffet i de andre stegene. På den måten er det mulig å få belyst spørsmålene om hvilke regulatoriske strategier (hovedregler, strukturer og språkbruk) som faktisk

virker (direkte eller indirekte), og hvilke som ikke gjør det. Det vil også være mulig å kartlegge regelverkens samlede effekt på realisert informasjonssikkerhet, effekten av andre virkemidler, etc. For eksempel vil det være mulig å beregne, hvis en virksomhet for eksempel får "høy score" på realisert informasjonssikkerhet, hvor stor andel av arbeidet som kan tilbakeføres til de rettslige reguleringene. Samlet vil dette gi et bedre og empirisk basert utgangspunkt for regelverksrevisjoner. Funnene fra de empirisk baserte undersøkelsene kan med andre ord i neste omgang gjøres om til potensielle styringsvariabler for lovgiver, regelverksforvaltere og tilsyn.

Det er ikke mulig her, heller ikke hensiktsmessig, å fastsette hvilke enheter som bør analyseres. Men hvis virksomheter som er konfrontert med rettslig kompleksitet brukes som utvalgs-kriterium, er antakelig de norske generalistkommunene aktuelle kandidater. Kanskje mer enn noen andre blir de eksponert for mangfoldet av regelverk om informasjonssikkerhet. De ansetter dessuten om lag 2/3 av alle ansatte i offentlig sektor, og egner seg godt komparative analyser. Ikke minst fordi det fra før er samlet inn omfattende bakgrunnsdata om kommunene som kan anvendes i studien for å forklare variasjon. Selvfølgelig vil det også være interessant å kartlegge konsekvensene av reguleringene for forskjellige grupper av virksomheter i næringslivet. Det vil dessuten være spennende å velge tilsvarende undersøkelsesenheter fra andre land, for eksempel fra Sverige eller Danmark. På den måten er det mulig å utvikle komparative analyser som kanskje viser variasjoner i regulatoriske strategier på tvers av landegrensene. Dette kan i neste omgang danne grunnlaget for ny kunnskap og læring om rettslige reguleringer av informasjonssikkerhet i Norge.

5.2.3 Behovet for å se nærmere på hvordan regler om informasjonssikkerhet samordnes og koordineres.

Det andre hovedgrepet Haug fremmer er å *se nærmere på hvordan regler om informasjonssikkerhet samordnes og koordineres*. Bildet som er presentert over av regelverkene om informasjonssikkerhet viser flere eksempler på dette. Dette gjelder ikke minst selve regelverkene (språkbruk, struktur, dokumentasjonskrav, etc.) men også alle tilsynsordningene og andre organisatoriske forhold. Det finnes flere alternative tilnæringsmåter. I Haugs studie gjengir han en del forenklet noen av ideene og forslagene til samordning av reglene fremsatt av Schartum (2004). Haug slutter seg til disse tankene, som en sentral vei videre. Schartum har utviklet dette videre i forbindelse med arbeidsgruppens arbeid, gjengitt i sin helhet i kapittel 5.1 foran. Haugs fremstilling i denne sammenhengen gjengis derfor ikke her.

5.3 Kort gjennomgang av anbefalinger om tiltak

Arbeidsgruppen setter pris på bidragene fra Schartum og Haug, og deres gjennomgang og forslag i 5.1 og 5.2. Arbeidsgruppen har ikke gått inn i eller god for alle enkeltheter ved verken innhold eller form; poenget er at dette er Schartums og Haugs tenkning og formuleringer. Arbeidsgruppen mener bidragene er av stor interesse for det videre arbeidet på området. Forslagene er konstruktive, og vi ønsker å stille oss bak forslagene. Disse er i stor grad

proessorienterte, og de nærmere detaljer må det tas stilling til underveis. I dette punktet har vi samlet en kortfattet fremstilling av våre forslag nedenfor, inkludert de nevnte.

5.3.1 Det settes i gang et kontinuerlig, systematisk og helhetlig arbeid – stikkord: ”regelverkssyklus og verktøy”

Aktiviteter:

- Det settes sammen en gruppe bestående av personer fra sentrale regelmyndigheter (forvaltere og de med operativt ansvar) og academia, (jf forslaget i 5.3.2 nedenfor). Gruppen får til oppgave å spesifisere krav til det som foran (i 5.1) betegnes som et ”verktøy”, dvs krav til et IKT-basert hjelpemiddel for bruk ved håndtering av sikkerhetsregelverk. Et slikt verktøy bør inneholde noen elementer på alle trinn i ”regelverkssyklusen” (jf avsnitt 5.1.3), og det er særlig grunn til å dekke evalueringstrinnet i den nevnte syklusen.
- Arbeidet bør starte ved at en arbeider med forholdsvis enkle prototyper som tidlig prøves ut for å vinne erfaringer. På den måten kan en sikre best mulig styring over faglig innhold og økonomi. Dersom det blir utviklet verktøy som regelmyndigheter ønsker å teste, bør slik bruk være gjenstand for forskning, for på den måten å fastslå faktiske effekter av verktøyet, og dermed vinne grunnlag for videreutvikling og videre bruk.
- Oppstart bør skje samtidig for alle regelverkene. Ansvaret ligger/forblir hos den enkelte myndighet.
- Et resultat av arbeidet med ”Verktøyet”/det IKT-baserte hjelpemiddelet vil/bør være at det (blant mye annet) lages en elektronisk kokebok/oppskriftsbok for forvaltere av regelverk: hvordan forvalte regelverket. ”Oppskriften” bør bygge på praktiske erfaringer, og selv være så praktisk som mulig, og følge regelverket i hele dets levetid, samt være helhetlig i forhold til regelverkets omgivelser.
- KIS kan være igangsetter av dette arbeidet, ut fra sin rolle og sitt ansvar, og påse at det skjer en samordning med videre i forbindelse med gjennomgangen.

Kort begrunnelse:

Arbeidet vil gi grunnlag for bedre samordning, koordinering og forenkling, og derved øke sannsynligheten for etterlevelse og styring i retning av god nok informasjonssikkerhet, som er regelverkernes mål.

Et resultat av dette arbeidet vil være at regelverket blir gjennomgått også med sikte på forenkling, dvs. opprydding av begreper, samordning av overlappende regler, evt. muligheter for sammenslåing, både pr sektorregelverk og regelverkene på tvers.

Et slikt arbeid gir etter arbeidsgruppens mening den mest lovende muligheten for å arbeide videre med de eksisterende sikkerhetsregelverkene, i en

kombinasjon av systemutvikling og forskning, og koblet direkte til det praktiske livs krav, ved at sentrale departementer og direktorater/tilsyn samarbeider med representanter fra akademia. Det forutsettes at også brukere involveres.

Det vil ta kort tid å starte opp et slikt arbeid og raskt oppnå delresultater. Delresultatene vil ha verdi i seg selv både direkte ut fra forvalter- eller tilsynsrollen i dagliglivet, og i et lengre og mer helhetlig perspektiv. Arbeidet vil ikke bare være metode- og produktorientert, men også prosessorientert, og fungere kontaktskapende for deltakerne (som har ansvar for de viktigste regelverkene for informasjonssikkerhet). Verdien vil være på både myndighets- og brukersiden. Arbeidet er ikke et engangsarbeid, men av løpende karakter, og må følge regelverkens livssyklus.

”Verktøyet” vil hjelpe regelverksforvaltere, og evt. tilhørende tilsyn, med bl.a. å følge opp sine regelverk på en systematisk måte, og herunder innhente opplysninger om

- Er regelverket kjent?
- Er regelverket i bruk/blir det fulgt?
- Hvilken effekt har regelverket i praksis?
- Hvis regelverket evt. ikke er kjent, i bruk/ikke blir fulgt, helt eller delvis - hvorfor? Hvis det ikke har ønsket effekt – hvorfor? Hva kan være relevante tiltak? Forslag til løsninger på et enkelt nivå bør finnes i den elektroniske ”kokeboken/oppskriften/verktøyet”.

5.3.2 Samarbeid for regelverks- og tilsynsarbeidet

Aktiviteter:

- Det etableres en arena/en møteplass/et forum/en gruppe for samarbeid mellom de mest sentrale myndighetene for regelverk og informasjonssikkerhet – både forvaltere og tilsynsmyndigheter. Dette blir en viktig møteplass for sentrale spørsmål rundt regelverk på området. Det bør holdes jevnlig møter – ut fra det rikelige tilfanget av aktuelle spørsmål knyttet til regelverk og informasjonssikkerhet.
- Deltakere på hvilket nivå? Det bør være på et nivå med tilstrekkelig ansvar og autoritet til å kunne komme med toneangivende forslag og tiltak, for å kunne påvirke utvikling og praksis. Spørsmål om å se helheten i samspillet mellom bl.a. organisatoriske, pedagogiske og juridiske virkemidler. Også ha et samarbeid med forskningsmiljøer på området.
- En slik møteplass/gruppe må behandle eller delta i en rekke aktiviteter, deriblant aktivitetene nevnt 5.3.1. I tillegg er mange andre temaer aktuelle. Blant disse er fokus på å få frem hva som er spesifikt for det enkelte regelverksområdet og hva som kan behandles felles/liket. Videre fokus på hva som kan dekkes ved å følge en eller flere standarder. Videre hva som eventuelt ikke dekkes og må håndteres i tillegg/særskilt. Jf NS 7799 og andre tilsvarende sikkerhetsstandarder, i forhold til personopplysningsforskriftens kapittel 2 (informasjonssikkerhet), e-

forvaltningsforskriftens § 13 (2) (om at sikkerhetsstrategien skal bygge på ”anerkjente prinsipper for informasjonssystemers sikkerhet”, osv).

- Det settes i gang konkret samarbeid mellom tilsynene, herunder utvikling av rutiner for samordning av tilsyn og (videre)utvikling av tilsynsmetodikk.
- KIS kan være igangsetter av dette arbeidet, ut fra sin rolle og sitt ansvar, og påse at det skjer en samordning med videre i forbindelse med gjennomgangen.
- Selvregulering: PT har gode erfaringer med uformelle arbeidsgrupper hvor tilsynet møter aktørene med formål å løse felles anliggende på en rask og smidig måte. Det kan settes ned Ad hoc arbeidsgrupper med representanter fra de ulike interessentene som kan komme opp med alternative løsninger et større ”brukerforum” kan ta stilling til. En slik fremgangsmåte er både tidsbesparende og demokratisk, og derfor ønskelig både fra tilsynenes og aktørenes side.

Kort begrunnelse:

Man har så vidt vi vet ennå ikke formalisert samarbeid mellom myndigheter med ansvar for regelverk og informasjonssikkerhet (departementer og tilsyn). Dette innebærer at det er de berørte virksomhetene/brukerne som selv må samordne kravene fra de ulike tilsynsmyndighetene og sikkerhetsregelverkene.³⁹ Økt kunnskap og samrøre på tvers mellom myndighetene kan bidra positivt til lettere hverdag for brukerne, bedre rettsanvendelse og etterlevelse fra brukerne, og mer effektiv håndtering fra myndighetene.

Det er grunn til å tro at det internt både i departementer og tilsyn med ansvar for regelverk på dette området er liten kunnskap om, og/eller fokus på, andre nasjonale sikkerhetsregelverk enn det som følger av egen virksomhet.

Samarbeid på tvers av tilsynene for å unngå ”dobbelttilsyn” vil være ressursbesparende for både tilsynene og aktørene. Tilsynene fører i mange tilfeller tilsyn med de samme bedriftene. Det er derfor ønskelig at tilsynene i størst mulig grad identifiserer overlappende oppgaver og i hvilken grad de for eksempel innsamler den samme informasjonen eller utfører stedlig tilsyn i de samme bedriftene. Innrapportert informasjon til offentlige myndigheter bør i størst mulig grad gjenbrukes.

³⁹ I *Veiledning lover og regler med betydning for informasjonssikkerhet, IT-sikkerhetsForum (ISF), versjon 1.0 mars 2003* står følgende treffende formuleringer: ”Så lenge regelverkene ikke koordineres der de utvikles, må koordinering skje der reglene etterleves – det vil si i den enkelte virksomhet. Målsettingen for virksomhetene bør/må uansett være å etablere én sikkerhetsløsning som tilfredsstillende flere/alle lovmessige sikkerhetskrav, i tillegg til de forretningsmessige og kontraktuelle kravene.” Dette kan stå som en kommentar til både det første (5.3.1) og det andre (5.3.2) tiltaksforslag over.

Samarbeid tilsynene imellom kan skje både på et formelt og på et uformelt plan. Det kan ofte være smidigere med uformell kommunikasjon. Imidlertid kan kontinuiteten da bli en utfordring. Det er viktig at samarbeidet settes i system. Man må også ta hensyn til at den innsamlede informasjonen i stor grad er sensitiv og at det av sikkerhetsmessige grunner kan være vanskelig å gi detaljert informasjon videre til andre tilsyn.

Ref: E-Norge. Tilsynsmeldingen. Forskriftsdugnaden

5.3.3 Bedre pedagogiske tiltak

Aktiviteter:

- Det settes i gang pedagogiske tiltak som kan ha nytte på tvers; formidling av god informasjon, opplæring, herunder e-opplæring/nettbasert læring, veiledninger, kurs, seminarer, konferanser. Målgruppe ikke bare brukere, men også myndighetene selv. Det må utvikles felles informasjonsmateriell og kommunikasjonskanaler til virksomhetene. Flere forvaltningsområder bør samarbeide, slik at det blir samordnet informasjon og budskap. Disse ressursene bør samordnes av myndighetene.
- Som inspirasjon, se det nyetablerte Nettvett (<http://www.nettvett.no/>). Dette er et meget godt tiltak som kan inneholde mye nyttig også for våre målgrupper. Det bør vurderes å lage en tilsvarende løsning for "våre målgrupper", i et samarbeid mellom de ansvarlige myndighetene for informasjonssikkerhet, og eventuelt i et samarbeid med Nettvett.no, som er laget av Post- og teletilsynet (PT) i samarbeid med andre myndigheter, IKT-bransjen og representanter for brukerne. Felles informasjon til felles brukere, som gir merverdi og helhet.
- Gode informasjonskanaler: Tilsynene bør sørge for gode informasjonskanaler både mot aktørene de fører tilsyn med og mot sluttbrukerne for å sikre kvalitet og pris på tjenestene og nødvendig kritisk masse. Gode innarbeidede informasjonskanaler bør også brukes til å informere om regelverket og utveksle informasjon. PT har gode erfaringer fra sine nettsteder Telepriser.no, Nettvett.no og Bredbandsporten.no
- Utvikle bransjerettet informasjon. Her bør man samarbeide med bransjen. Hvilke bransjer er aktuelle? Se Hammer s. 36 – bransjespesifikke krav, se eks. på bransjer s. 33) Kan videreutvikles til bransjenormer. Se også forslaget fra PT om selvregulering i 5.3.2 sjette kulepunkt, foran. Bransjen blir enig om hvordan den skal etterleve regelverket. Det kan også innebære at man stiller strengere krav til seg selv enn det som er nødvendig for å etterleve regelverket.
- Videreutvikle og samordne eksisterende nettportaler om informasjonssikkerhet (hjelp for brukerne).

- Utvikle nettbasert opplæring (jf nærmere omtale av hva nettbasert opplæring kan være i vedlegg 7 til rapporten) for hvert av regelverkene for informasjonssikkerhet for brukerne, som kan være tilgjengelig 24/7, og så ofte en bruker har behov for å komme tilbake til den. Opplæringen bør også vektlegge å se sammenhengen/grenseflater til andre regelverk om informasjonssikkerhet. Laget av regelverksansvarlig og tilsyn i samarbeid, bygget på deres kombinerte kompetanse, og løpende oppdatert ut fra deres systematiske erfaringsinnhenting og utviklingen for øvrig.
- Det må utarbeides, ajourføres og bearbeides videre veiledninger/kommentarutgaver til de ulike regelverkene, uansett valg av medium (papirbasert eller elektronisk/nettbasert). Spesielt behov når det gjelder regelverk som ennå ikke har noe veiledning, eksempelvis beskyttelsesinstruksen.
- Det må lages en veiledning som tar for seg berørte flater mellom regelverk om informasjonssikkerhet og andre relevante regelverk (offentlighetsloven, forvaltningsloven, personopplysningsloven, eSignaturloven, osv).
- Kravmottakere/brukere vil vite hva de må gjøre konkret i tillegg til å tilfredsstillende ”anerkjente standarder”. Slik oversikt bør lages av regelverksforvaltere som stiller krav om å følge anerkjente standarder, og lover at da er man ”nesten i mål” i forhold til regelverket. Hvor nesten er nesten?

Kort begrunnelse:

Behovet kan variere noe fra regelområde til regelområde. Men generelt kan en si at det er et skrikende behov for pedagogiske tiltak for å få regelverkene til å virke etter hensikten. Det er ikke tilstrekkelig å vedta regler, man må også ta i bruk formidling og andre gode pedagogiske virkemidler på en systematisk og kontinuerlig måte, i regelverkets levetid. Dette er nødvendig både for å oppnå den styrings- og påvirkningseffekten som myndighetene er ute etter, og for å gjøre det mulig for ”folk flest” å etterleve kravene fra ett eller flere regelverk. De fleste regelverkene i vår sammenheng har veiledninger knyttet til seg i større eller mindre grad. Disse kan vurderes forbedret ytterligere. Særlig ved krav fra flere regelverk samtidig, bør det legges stor vekt på de pedagogiske sider for å hjelpe brukerne. Dette er i dag lite utviklet, eller ikke i det hele tatt. Nettbasert opplæring er et virkemiddel som heller ikke er tatt i bruk ennå på dette området (så vidt vi vet), og som kan stå i nært forhold til forslaget om å utvikle tenkning/sette i gang konkret arbeid i retning av ”regelverkssyklus og verktøy”, jf 5.3.1 ovenfor.

Ref: Forskriftsdugnaden

5.3.4 Vurdere effekter av regelverket, empiri, evalueringer - etterkontroll

Aktiviteter:

- Det må fremskaffes et *bedre empirisk basert beslutningsgrunnlag for det videre arbeidet*. Hovedutfordringen ligger i å utvikle et forskningsteoretisk utgangspunkt for en empirisk drevet videreutvikling av regelverkene om informasjonssikkerhet. Deretter bør det gjennomføres tester av effekten av reglene på et utvalg relevante virksomheter. Kanskje kan den instrumentelle virkemiddelmodellen som er presentert i kapittel 4 i Haugs utredning anvendes som et utgangspunkt, men ytterligere operasjonaliseringer er nødvendige.
- Det bør gjennomføres konkrete studier (eksempelprosjekt) av representative virksomheters håndtering og etterlevelse av krav fra ett eller flere regelverk om informasjonssikkerhet (stat, fylkeskommune, kommune, stor næringsvirksomhet, mellomstor og liten næringsvirksomhet – andre?). Vurdere tiltak og lære av og spre erfaringer. Et ønsket og etterspurt resultat av dette vil være eksempler og maler som vil være lette å ta bruk for brukerne.
- Regelverket bør systematisk evalueres/etterkontrolleres for å finne ut hvordan reglene faktisk virker (effekter). Kontrollen skal danne grunnlag for evt. behov for innholdsmessige/materielle endringer, evt. også ytterligere endringer av begreper, språk og struktur. I tillegg kan/bør andre virkemidler vurderes.
- Det må vurderes om evalueringen skal omfatte de enkelte sektorene hver for seg, eller om det i tillegg skal være tverrgående evalueringer. Analysen skal danne grunnlag for iverksetting av tiltak.
- Vurdere nye/alternative virkemidler for etterlevelse av regelverket, herunder økonomiske virkemidler som sertifiseringsordninger.
- Bruke verktøy og metoder for informasjonsinnhenting. Dette kan være å opprette nettportal med info om regelverk for informasjonssikkerhet ("verktøyet" omtalt foran i 5.1 og 5.3.1) – for myndighetene. Hvordan utnytte dette verktøyet mht. evaluering i praksis? Bør resultere i en felles mal som myndighetene kan bruke, og hvor det er rom for sektortilpasninger. En gruppe med representanter fra tilsynsmyndighetene bør nedsettes. Herunder vurdere utvikling av verktøy for nettbasert veiledning til brukerne, også basert på bl a spørsmål/svar. Info brukes som en del av myndighetenes informasjonsinnhenting.
- Det bør utarbeides noen sentrale retningslinjer/sjekkliste/rutiner for evalueringen

Begrunnelse:

Det er en grunnleggende svakhet ved dagens regelverk og forvaltningen av dem at man ikke systematisk undersøker hvilken effekt regelverkene har. Når en tenker på hvilke vekt samfunnet legger på å styre ved hjelp av rettsregler, burde

det også være av interesse å gjøre mer for å finne ut av om rettsreglene er kjent, virker etter hensikten osv. De enkelte tilsyn gjør i dag en innsats for å bedre etterlevelsen. Det bør i tiden fremover legges økende vekt på tilsynene som viktige elementer for å samle betydelig bedre empiri på en systematisk måte, som også kan ses på som forberedelse til/innsjutt til eventuell evaluering og forbedring av regelverket, jf forslagene foran om "regelverkssyklus og verktøy" i 5.1 og 5.3.1.

Ref: Are Vegard Haugs studie, (kap 5.2 og vedleggene 1 og 4, samt fremstillingen til Dag W. Schartum i nevnte 5.1 og derav følgende forslag i 5.3.1.

5.3.5 Andre tiltaksforslag

- Regelverk bør så langt som rimelig/mulig tuftes på samme underlag, for eksempel ISO 17799. Det bør lages eksempelprosjekt med konkrete virksomheter, for å vise hvordan de kan nyttiggjøre seg en eller flere standarder, i forhold til etterlevelse av regelverk om informasjonssikkerhet.
- Vurdere om flere regelverk bør henvise til /bygge på standarder som minstekrav for oppfyllelse av kravene i regelverkene.
- Det kan lages sjekkliste eller veiledning for egenrevisjon/internkontroll mht etterlevelse av regelverk om informasjonssikkerhet.
- Det bør utvikles et krav om at virksomheter som er underlagt regelverk om informasjonssikkerhet må rapportere i årsmeldingen sin om hvordan dette håndteres konkret det enkelte år, sett i forhold til regelverkens krav og de forretningsmessige eller forvaltningsmessige målene virksomheten har, der risikonivået må være tilpasset dette. Viktig for å engasjere ledere for virksomheten, som ellers ikke engasjerer seg i informasjonssikkerhet (eksempelvis rådmenn i kommuner). En slik ledelseserklæring kan med fordel ledsages av et krav om bekreftelse fra uavhengig tredjepart (om samsvar mellom erklæringen og virkeligheten).⁴⁰
- Det bør kunne utvikles en forskrift som dekker temaet informasjonssikkerhet – sektoruavhengig. Grunnprinsippet bør være forholdsmessighet. I den grad det kan påvises særskilt behov gis tilleggskrav innen nærmere angitte områder.
- Det bør gjøres et forsøk på å samordne/lage en felles forskrift på de områdene dette er mulig – noe som først og fremst vil gjelde i forhold til sikkerhetsadministrasjon. Dette regelverket bør være et felles

⁴⁰ (Deler av dette forslaget er inspirert av intervju med styret i KINS (Statskonsult, internt notat 2004-12-07), og deler av det av Lars Erik Fjørtoft, se hans mer omfattende forslag i vedlegg 6 til rapporten).

utgangspunkt for ethvert arbeid med informasjonssikkerhet. Videre krav til sikring må være avhengig av skjermingsbehov og risiko.

- Myndighetene bør slik kunne oppdage hverandre og samarbeide, og brukerne har ett sted som innfallsport for å oppdage hvilke regler som gjelder for dem. Og kan få veiledning og hjelp på mange ulike måter via nettside opprettet for formålet.
- Det bør ryddes opp i forholdet mellom sikkerhetsloven og beskyttelsesinstruksen.
- Økonomiske virkemidler: Det bør vurderes å ta i bruk økonomiske virkemidler. Eksempelvis: gjøre det mer attraktivt å bli sertifisert! Det bør bety noe "lønnsomt" å være sertifisert. Kan være en god investering fra samfunnets side å bruke slike lokkemidler - i hvert fall i en fase av utviklingen hvor det går tregt.
- Det bør vurderes å innføre en form for økonomisk gulrot for å følge anerkjente standarder (jf krav i flere regelverk)

Det finnes flere tiltaksforslag som bør vurderes i det videre arbeidet. Se tiltaksforslagene fra andre, høyst meningsberettigede i vedlegg 6 (IT-Sikkerhetsforum, ISF, og leder av ISFs regelverksarbeid, Lars Erik Fjørtoft, samt Johs. Hansen Hammer).

Se også vedlegg 7, om å Påvirke holdninger og kunnskap ved nettbasert læring, der det gis en kort oversikt over hva dette kan innebære.

Vedlegg

Følgende vedlegg finnes i eget vedleggsnotat til arbeidsgruppens rapport:

Vedlegg 1: Are Vegard Haug: Oversikt over rettslige reguleringer av informasjonssikkerhet (sektorperspektiv); Kapittel 5 som finnes i Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet, AFIN, UiO (under ferdigstilling mai 2005)

Vedlegg 2: Johs. Hansen Hammer: Informasjonssikkerhet. Risikostyring – metoder og verktøy. En vurdering av egnethet for SMB, kapittel 6 (2004)

Vedlegg 3: Oversikt over lover/forskrifter som gjelder kraftleverandørbransjen (Statnett)

Vedlegg 4: Are Vegard Haug: Analyser av de rettslige reguleringene av informasjonssikkerhet; Kapittel 6 som finnes i Rettslige reguleringer av informasjonssikkerhet. Mot instrumentelle virkemiddelmodeller innen juridisk forskning på informasjonssikkerhet, AFIN, UiO (under ferdigstilling mai 2005)

Vedlegg 5: Evaluering av regelverk – ett eksempel. Sammendrag av evaluering av eForvaltningsforskriften, Rapporter fra Statskonsult på oppdrag fra Moderniseringsdepartementet 2004

Vedlegg 6: Enkelte kommentarer og forslag fra andre

Vedlegg 7: Påvirke holdninger og kunnskap ved nettbasert læring

Litteraturliste

NOU 1986:12 Datateknikk og samfunnets sårbarhet (Seiputvalget)

Samordning av regelverk for beskyttelse av informasjon. Rapport fra arbeidsgruppe (FD, JD, AAD 1991)

NOU 2000:24 [Et sårbart samfunn. utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet](#) (Willochutvalget)

NOU 2001:4 [Helseopplysninger i arbeidslivet. Om innhenting bruk og oppbevaring av helseopplysninger i arbeidslivet](#)

To rapporter om evaluering av forskrift om kommunikasjon med og i forvaltningen (Statskonsult for Moderniseringsdepartementet 2004)

Rapport om departementenes arbeid med informasjonssikkerhet (Riksrevisjonen, kommer våren 2005)

Annen relevant litteratur om informasjonssikkerhet

Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur
vurdert i lys av ønsket om samordning (Dag Wiese Schartum 2005)

Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT (Arild Jansen, Dag
Wiese Schartum (red), Fagbokforlaget 2005)

Veiledning. Lover og regler med betydning for informasjonssikkerhet (IT-
sikkerhetsforum, mars 2003)

Informasjonssikkerhet. Risikovurdering og sikkerhetsstyring – metoder og
verktøy (En utredning for Nærings- og handelsdepartementet av Johs. Hansen
Hammer, august 2004)

Relevante arbeider om forenkling og samordning av regelverk generelt

NOU 1992:32 Bedre struktur i lovverket

Forskriftsdugnaden. Prosjekt for opprydding i og forenkling av forskriftsverket
(Nærings- og handelsdepartementet og Justisdepartementet 2002)

Om forenkling av regelverk (Kristin Kjelland-Mørdre, CompLex 12/83,
Institutt for rettsinformatikk, UiO)

EDB – Mulighet og problem ved forenkling av regelverk (Jon Bing, CompLex
12/83, Institutt for rettsinformatikk, UiO)

Rettsregler, rettsinformasjon og regelreform (Brynjar Mørkved, Nordisk
Administrativt Tidsskrift 2/1991)

Kartleggingsprosjektet. Kartlegging av bestemmelser i lover, forskrifter og
instrukser som kan hindre elektronisk kommunikasjon, Nærings- og
handelsdepartementet 2000)

Stat & Styring nr 1/2005:

Tilsyn utviklet frivillig en felles profil, s. 3

Sterk kritikk av manglende samordning, s. 9