Notater om å ivareta informasjonssikkerhet ved hjelp av regelverk

Professor dr. juris Dag Wiese Schartum, Avdeling for forvaltningsinformatikk (AFIN), UiO[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 arbeider, men prøver å se på spørsmål vedrørende regelverk for sikring av informasjon med "friske øyne". Samtidig er det imidlertid klart at deler av notatet er inspirert av resultater fra andres arbeid. Særlig gjelder dette arbeidet som forsker Are Vegard Haug ved Avdeling for forvaltningsinformatikk har utført vedrørende kartlegging og diskusjon av sikkerhetsregelverk.[2]

I første avsnitt av notatet diskuterer jeg hva informasjonssikkerhet og informasjons-sikkerhetsregelverk 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 informasjons-sikkerhetsarbeidet som bør prioriteres. I avsnitt 3 skisserer jeg en modell for regelverksarbeid som etter min mening er anvendelig for arbeidet med sikkerhetsregelverk. Denne modellen forutsetter bruk av teknikker, verktøy og organisering som virkemidler i de ulike trinnene i arbeidet med regelverk. Regelverk som pålegger plikter eller innskrenker rettigheter og som dessuten er ressurskrevende å etterleve for "pliktsubjektene" vil lett skape motsetningsforhold. I avsnitt 4 gjør jeg en enkel beskrivelse av mulige hovedmotsetningsforhold i sikkerhetsarbeidet, og antyder noe om mulige implikasjoner for valg av reguleringsstrategi. I avsnitt 5 drøfter jeg med bakgrunn i slike eventuelle motsetninger, og mulige implikasjoner for utforming av regelverk som kan sikre mest mulig effektiv styring (avsnitt 5). Resten av notatet (avsnittene 6 – 8) inneholder skisser av slik virkemiddelbruk som jeg forutsetter i modellen for regelarbeidet i avsnitt 4. Stikkord her er teknikker for samordning av regelverk (avsnitt 6), verktøy for forarbeider, regelanvendelse og evaluering (avsnitt 7), og organisering av rettsanvendelsen (avsnitt 8). Avslutningsvis gir jeg noen råd om det videre arbeidet med informasjonssikkerhetsregelverk.

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

2 Allment om regelverk vedrørende informasjonssikkerhet

Informasjonssikkerhetsregelverk betegner – naturlig nok – regelverk som skal sikre informasjon. Noen ganger brukes også betegnelsene "datasikkerhet" og "datasikkerhets-regler". Ut i fra et vanlig skille mellom informasjon og data, kan det være naturlig å legge

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

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

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

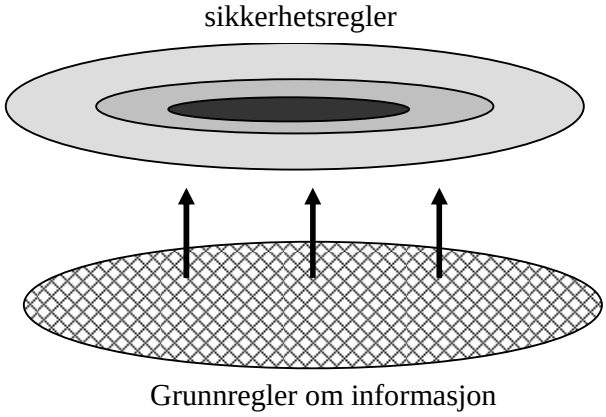
"Sikkerhet" og "sikring" kan selvsagt også gjelde annet enn informasjon. Sikkerhet kan for eksempel gjelde helse- og miljø, brann- og eksplosjon, trafikk/transport, el-forsyning osv. Selv om slike sikkerhetsspørsmål i utgangspunktet utgjør selvstendige områder, er det viktig å understreke at informasjonssikkerhet er innvevd i disse andre sikkerhetsområdene. Fordi informasjonssystemer styrer sentrale prosesser på nær sagt alle livsområder, vil det ofte være 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 en etterlevet. Lovgivningen stiller for eksempel opp bestemmelser om taushetsplikt, mens sikkerhetsregelverket stiller krav til informasjonsbehandlingen som øker sannsynligheten for at taushetsplikten blir effektiv (passordbeskyttelse, brannmur, loggføring mv). På lignende måte stiller (bl.a) offentlighetsloven opp krav til innsyn i offentlige saksdokumenter, mens sikkerhetsregler stiller krav som øker sannsynligheten for at folk faktisk kan få tilgang til de opplysningene de har krav på å se (krav om reservekopiering, "oppetider" for informasjonssystemet mv).

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

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

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



Figur 1: Samspillet mellom grunnregler og sikkerhetsregler

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

Midterste sone betegner sikkerhetsregler i form av mer enkeltstående bestemmelser, dvs bestemmelser som løser konkrete problemer, for eksempel som respons på en uheldig hendelse eller lignende.[6] Begge disse kategoriene representerer eksplisitt regulering av informasjonssikkerhet, fordi kravet om sikring går direkte frem av rettsreglene. I ytterste sone av figuren finner vi imidlertid "implisitt" regulering av sikkerhet, dvs der det ikke sies i klartekst at sikkerhetstiltak skal treffes, men hvor dette følger indirekte av regler i lov eller forskrift eller av uskrevne rettslige prinsipper. Det viktigste eksempelet på siste kategori er grunnregler i kombinasjon med internkontrollbestemmelser, dvs bestemmelser som pålegger rettssubjektene å vurdere om det er behov for å iverksette tiltak for å sikre etterlevelse av rettsregler for øvrig. Kombinasjonen av internkontrollbestemmelser og grunnregler som stiller krav til konfidensialitet, integritet og tilgjengelighet, kan med andre ord ses på som sikkerhetsbestemmelser. På lignende måte kan for eksempel prinsippet om forsvarlig saksbehandling i kombinasjon med regler som gir krav på tilgang til informasjon, innebære en forpliktelse til å iverksette tiltak for å sikre slik tilgang. Etter offentlighetsloven bestemmer forvaltningsorganet innenfor rammene av krav til forsvarlig saksbehandling hvorledes gjennomføringen av innsyn skal skje. Dersom krav til forsvarlig saksbehandling tilsier det, må de med andre ord treffe tiltak som sikrer tilgjengeligheten.

Denne tredelingen av feltet informasjonssikkerhet, viser både noe om mangfoldigheten av den relevante rettslige reguleringen, og omfanget av de reguleringer som med rimelig grunn kan hevdes å være del av den familie av rettsregler som vi kan si gjelder informasjonssikkerhet. I et videre arbeid med sikte på å forbedre den rettslig regulering av informasjonssikkerhet, er det neppe hensiktsmessig å oppta seg med alle tre "soner". Etter mitt syn er det – i alle fall initialt – grunn til å legge avgjørende vekt på de helhetlige informasjonssikkerhets-regelverkene. 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

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

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

regelverk vedrørende informasjonssikkerhet, også vil kunne ha positive effekter for øvrig relevant regelverk.

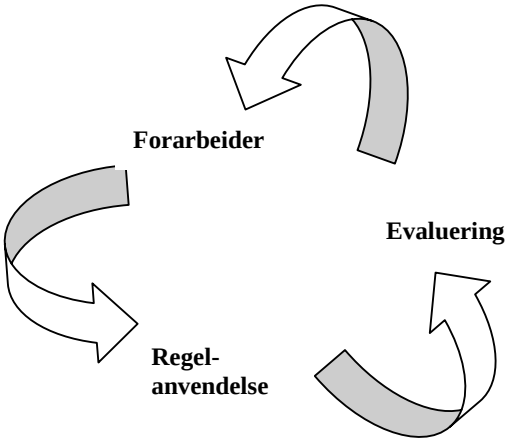
Dersom vi ser på de grunnreglene om informasjon som bestemmelser om informasjonssikkerhet skal ivareta etterlevelsen av, er dette konvensjonelt krav vedrørende konfidensialitet, integritet og tilgjengelighet. En kan imidlertid tenke seg sikkerhetsregler som skal ivareta etterlevelsen av flere andre grunnregler; 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).[7] En helhetlig tilnærming til informasjonsbehandling kan tilsi at dette er en hensiktsmessig løsning. Dersom en imidlertid ser på hva slags kompetanse som kreves for å ivareta de ulike elementene i kravene til sikring, kan det være en kommer til motsatt resultat. Sikring av konfidensialitet, integritet og tilgjengelighet er i stor grad noe som kan sikres gjennom fysiske, tekniske og teknologiske tiltak, og i tillegg "organisatoriske" tiltak vedrørende systemarkitektur, konfigurering av systemet mv. Slike spørsmål kan håndteres av "teknologer", og disse spørsmålene oppstår i tilknytning til ethvert informasjonssystem. Derfor er dette "globale" informasjonssikkerhets-spørsmål.

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

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

3 Helhetlig blikk på regelverksarbeid

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



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 hensikts-messighetsspørsmål som må vurderes konkret.

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

- organisering,
- metodikk og
- verktøy.

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

4 Motsatte perspektiver på regelstyring av informasjonssikkerhet

Et helt grunnleggende spørsmål er *hvorfor* vi skal introdusere og/eller forbedre regelverk om informasjonssikkerhet. Her vil jeg velge et enkelt og kanskje litt retorisk grep ved å spørre om det er effektiv styring eller "brukervennlig" regelverk vi vil ha? Dette er selvsagt en for enkel og firkantet problemstilling, men den er etter min mening nyttig for å identifisere noen mulige motsetningsforhold som det kan være en utfordring å håndtere når informasjons-sikkerhetsregelverk skal etableres eller endres. Et innledende poeng er i alle fall at det neppe er grunn til å anlegge en snill harmonimodell der alle gode ønsker settes side ved side uten å undersøke i hvilken grad det er mulighet for konflikter. Mitt utgangspunkt er at det er legitime og gode grunner til både å ønske mer effektiv styring av informasjonssikkerheten *og*

til å regulere sikkerhetsspørsmålene på en måte som er i bedre harmoni med de berørte personenes og virksomhetenes ønsker ("brukervennlig"). Poenget er imidlertid at sannsynligheten er stor for at det – i alle fall under visse omstendigheter – er konflikt mellom disse målsettingene. Derfor er det trolig ikke mulig å ta hensyn til begge mål uten å gjøre avveininger og modifikasjoner av utgangspunktene. Dette betyr likevel ikke at det alltid vil være motstridende interesser. Samtidig som det er grunn til å anta at det vil forekomme konflikter, er det grunn til å anta at det vil forekomme interessesammenfall. Konfliktene kan imidlertid antas å være av størst interesse fordi det er på slike punkter at regelverkets effektivitet settes på den største prøve. Det er derfor i slike spørsmål virkemiddelbruken i "regelverkssyklusen" må være mest intens og overveiet, jf forrige avsnitt.

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

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

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

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

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

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

Selv om motsetningsforholdet mellom de to perspektivene er 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 Kommunikasjon av sikkerhetsregelverk

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

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

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

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

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

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

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

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

ofte bør vurderes å tilpasse reguleringen til hva det faktisk er mulig å kommunisere og iverksette.

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

Sikkerhetsreglene inngår i "egne" regelverk
En viktig og grunnleggende erkjennelse er at de fleste som forventes å etterleve sikkerhetsregelverk ikke er jurister. Denne enkle kjensgjerningen har flere viktige implikasjoner. En mulig konsekvens er at deres kunnskap om 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 avvising av muligheten for å plassere bestemmelser om informasjonssikkerhet knyttet til eksisterende generell lovgivning dersom denne må antas å være alminnelig kjent. Innen offentlig sektor er for eksempel lovgivningen bygget opp under forutsetning av at berørte personer både kjenner den aktuelle særlovgivningen og felles rettsregler i forvaltningsloven, offentlighetsloven og personopplysningsloven. Antagelsen om at sikkerhetsregler bør inngå i kjente regelverk for å kunne bli godt kommunisert, kan imidlertid uansett være et moment som taler mot rettslig regulering som verken er knyttet til særlovgivning eller til eksisterende, sentral felleslovgivning.

På basis av disse betraktningene, kan det formuleres følgende antagelser om at sikkerhetsregler fortrinnsvis bør plasseres i forhold til følgende prioriterte rekkefølge:
1. Særlovgivning for det aktuelle virksomhetsområdet.
2. Felles, sentral lovgivning.
3. Annen lovgivning, eventuelt ved etablering av nytt regelverk som er uavhengig av 1) og 2).

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

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

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

Krever forhåndskunnskaper som adressatene har
En nærliggende antagelse er at det er lettere å kommunisere et regelinnhold på en vellykket måte dersom innholdet 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 innebære en utfordring mht intern ledelse og koordinering.

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

Reglene er beskrevet som en arbeidsprosedyre
Det å forstå en regeltekst innebærer å skjønne hvorledes regelmyndigheten ønsker at vi skal forholde oss, fordi etterlevelse av rettsregler innebærer at vi må utføre noen handlinger. Problemet med å omsette ord til handling, handler bl.a. om å forstå hva som er "prosedyren". Regelverk er ofte fragmentarisk ved at det er formulert regelfragmenter som den enkelte regelanvender selv må sette sammen for å forstå hvorledes han skal forholde seg. Anvendelse

av et fragmentert regelverk krever imidlertid generell problemforståelse og en viss juridisk kompetanse som en ikke uten videre kan forvente at den enkelte som skal etterleve sikkerhetsbestemmelsene har. Det kan derfor være grunn til eksplisitt å angi en prosedyre, dvs den konkrete fremgangsmåten som må følges for å nå et tilfredsstillende resultat: For den som kan lage sukkerbrød, er det nok å få oppgitt hva ingrediensene skal være og vedkommende vil vite at det må følges en helt spesiell fremgangsmåte for å få et vellykket resultat. Uten denne kunnskapen, er det gode muligheter for et mislykket resultat selv om alle ingredienser er kjent med nøyaktige mål. På lignende måte kan en det være vanskelig å etterleve et sikkerhetsregelverk selv om alle "ingredienser" er kjent, dersom regelverket ikke samtidig er klart vedrørende rekkefølgen på utførelse av de ulike arbeidsstegene som loven gir anvisning på.

Vektlegging av arbeidsprosedyre innebærer en antagelse om at det er størst mulighet for vellykket kommunikasjon av sikkerhetsregelverk, dersom dette legger vekt på tydelige angivelser av tid/rekkefølge og relasjonene mellom de ulike regelelementene. Dette innebærer 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 regelelementene. 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.

6 Samordning av sikkerhetsregelverk

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

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

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

personopplysningsforskriften fordi dette vil kunne igangsette parallelle forskriftsarbeider også på andre felt.

Jeg skal ikke her gå nærmere inn på en argumentasjon for eller i mot samordning av sikkerhetsregelverk. Før en slik vurdering kan skje, er det uansett grunn til å undersøke noe nærmere hva "samordning" kan tenkes å innebære. Nærmere analyse viser at begrepet samordning ikke gir noen klare svar i seg selv, og at det er en rekke mulige samordningstiltak å velge mellom. I det følgende vil jeg kort gjennomgå noen hovedalternativer. Alternativene er hentet fra min artikkel " Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning".[9] I artikkelen blir mulige samordningsteknikker identifisert og supplert med utgangspunkt i det sentrale norske sikkerhetsregelverket.

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

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

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

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

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

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

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

Felles skjønnskriterier og rettslige standarder. I tillegg til felles begrepsapparat i form av legaldefinisjoner mv, kan det være aktuelt å gjøre bruk av felles kriterier for skjønnsutøvelse eller rettslige standarder ("tilfredsstillende sikkerhet", "akseptabel risiko" mv). At vurderingene er knyttet til de samme kriterier, vil trolig innebære at vurderingene blir mer enhetlige enn om forskjellige kriterier hadde vært anvendt. Dersom samordningseffekten skal bli merkbar, vil dette imidlertid trolig kreve ytterligere tiltak, for eksempel bruk av felles verktøy eller lignende, jf nedenfor i avsnitt 4.

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

Felles regelverksarkitektur. Med "regelverksarkitektur" sikter jeg til måten regelverk er bygget opp på, og en felles regelverksarkitektur vil si at regelverkene er konstruert på likeartete måter. Arkitekturen gjelder primært de bærende delene av strukturen, snarere enn innholdet. Felles arkitektur kan for eksempel gjelde felles fordeling av bestemmelser mellom

lov- og forskriftsnivået, felles inndeling av regelverk i kapitler, felles rekkefølge på (typer av) bestemmelser osv. Slik felles struktur kan altså tenkes uavhengig av om det er noen form for innholdsmessig samordning. Fremgangsmåten kan gjøre det lettere å orientere seg i ulike regelverk vedrørende informasjonssikkerhet fordi den felles arkitekturen kan skape en felles forventning til hvorledes slike regelverk skal være bygget opp.

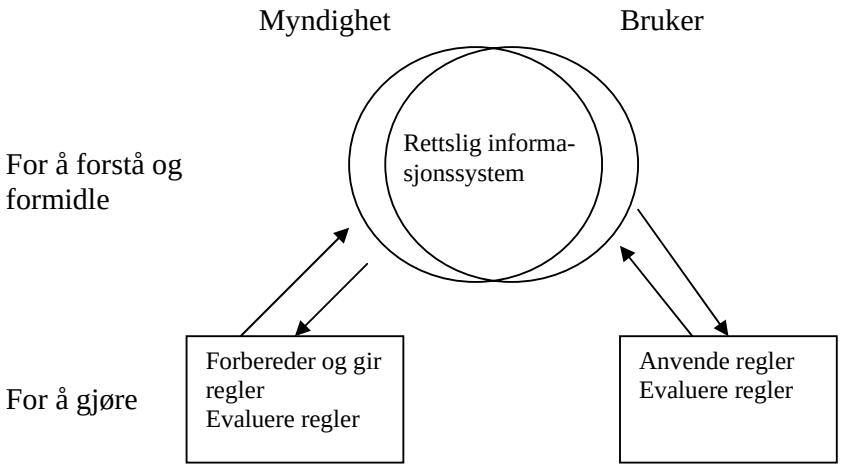
I tillegg til de 9 tilnærmingene til bedre samordning av informasjonssikkerhetsregelverk som jeg har nevnt ovenfor, er det flere mulig supplerende strategier som kan lede til bedre sammenheng mellom slike regler. Dette er med andre ord ikke fremgangsmåter som direkte gjelder utformingen av regelteksten,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

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

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

7.1 Innledning

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



Figur 3: Grunnleggende struktur for mulige verktøy knyttet til sikkerhetsregelverk.

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

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

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

7.2 Verktøy for utarbeiding av sikkerhetsregelverk

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

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

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

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

I de aktuelle regelverkene bør en også innarbeide alle eksplisitte henvisningsstrukturer slik at det er lett å studere den sammenheng hvert regelverk/hver enkeltregel står i. Dette gjelder for det første internt i et 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 7.4.

7.3 Verktøy ved anvendelse av sikkerhetsregelverk

Verktøy for anvendelse av sikkerhetsregelverk bør ses i nøye sammenheng med verktøy for utarbeiding og evaluering av regelverk, jf neste avsnitt. Det er særlig to mulige 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.[11] Kommentarene skal sette den enkelte bruker i stand til å lese og forstå de aktuelle rettsreglene. Dette innebærer at det for det første bør være kommentarer som er begrunnet i regelmyndighetens behov for å forklare og 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 anses å være nødvendig eller nyttig for å illustrere konkrete anvendelser av bestemmelser. Eksemplene kan gjerne følge samme mønster som kommentarstrukturen og eventuelt være en integrert del av denne. Det betyr blant annet at enkelte eksemplifiseringer kan gjøres i utgangspunktet, mens supplerende eksempler kan gis som respons på spørsmål som oppstår i tilknytning til bruk av regelverket. Et tredje element kan være å gjøre tilgjengelig autorative avgjørelser vedrørende fortolkning av bestemmelser i regelverket. Særlig er domsavgjørelser og avgjørelser i klagesaker aktuelle.

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

Det er selvsagt ikke slik at tekst- og funksjonsrettede verktøy nødvendigvis er alternativer. Tvert i mot bør et funksjonsrettet verktøy alltid være koplet til tekstrettede moduler. Dette fordi de underliggende rettskildene ikke bør fortrenges av systemløsningen. Tekstrettende verktøy kan imidlertid lettere aksepteres alene. Dersom en har en ekstensiv regulering slik at deler av regelverket forutsetter kunnskap som mange av de som skal følge regelverket ikke

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

kan antas å ha, kan dette være et argument for å legge vekt på å utvikle funksjonsrettet verktøy med høy automatiseringsgrad.

7.4 Verktøy ved evaluering av sikkerhetsregelverk

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

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

7.5 Avsluttende bemerkninger om verktøy

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

8 Organisering av rettsanvendelse

Den siste skissen av virkemiddelbruk på de ulike trinnene i regelverkssyklusen (jf avsnitt 3), gjelder organisering av rettsanvendelsen. Poenget er da at organiseringen av rettsanvendelsen skal tilrettelegge for det neste trinnet, dvs for evalueringen av regelverket. Organisering av rettsanvendelsen ellers vil primært være et spørsmål om å organisere saksbehandlingsarbeidet hos det forvaltningsorganet som har kompetanse på vedkommende fagområde på en måte som gir effektiv ressursbruk, rettsriktige resultater og forsvarlig skjønnsutøvelse. Slike hensyn er åpenbart viktige og legitime, men er knyttet til 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 7.3 kan ha slike organiserende effekter; Dvs verktøyet blir gjort attraktivt for flest mulige brukere av regelverket, og det legges til rette for fortløpende svar på tolkningsspørsmål mv (noe som kan motivere og øke bruken). Når en når frem til selve evalueringsfasen vil det foreligge et rikt "historisk" materiale. Dette kan suppleres i form av et retrospektivt materiale, dvs materiale som fremkommer ved at en undersøker tidligere saksforhold og begivenheter og spør om hva involverte personer har av hukommelse og oppfatninger.

9 Avsluttende bemerkninger

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

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

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