Regulering av informasjonssikkerhet

Til bolken "Forskning om rätt och säkerhet",
XX:e Nordiska rättsinformatikkonferensen, Stockholm 21. – 22. oktober

Professor Dag Wiese Schartum, AFIN, Universitetet i Oslo

I mitt innlegg vil jeg se nærmere på behov for forskning vedrørende de regulatoriske valg som gjøres for å fremme informasjonssikkerhet, og spesielt behovet for å evaluere om den rettslige reguleringen er effektiv og hensiktsmessig. Ved AFIN har forsker Are Vegard Haug nylig påbegynt prosjektet " Mapping Statutory Regulations of Information Security in Norway". Dette er første del av et treårig prosjekt der spørsmål vedrørende den eksisterende reguleringen av informasjonssikkerhet vil bli belyst. Prosjektet er finansiert av Norges forskningsråd under programmer IKT, sikkerhet og sårbarhet. Mitt innlegg vil gjelde Haugs problemområde, men uten at jeg tar mål av meg til å presentere dette spesifikke prosjektet.

For å forstå dagens norske situasjon er det viktig å kjenne litt til forhistorien. Veldig kort fortalt ble spørsmål om informasjonssikkerhet og sårbarhet diskutert gjennom meget av 1980-årene, og det ble nedlagt et ganske betydelig arbeid for å etablere et felles og enhetlig regelverk om informasjonssikkerhet. Denne prosessen kuliminerte med fremleggelsen av forslag til lov og forskrift om informasjonssikkerhet i 1992, men forslaget møtte så mye motstand at det aldri ble vedtatt. Etter at den store planen for samordnet regulering kollapset, har det imidlertid vært betydelig aktivitet på lovgivningsfronten, og vi har ut over 1990-tallet fått flere viktige regelverk som er ment å ivareta informasjonssikkerhet. En oversikt over de viktigste sikkerhetsregelverkene ser slik ut:

1992
- **Forskrift om informasjonsteknologi** med hjemmel i kredittilsynsloven; i 2003 revidert og vedtatt som forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (forskriften inneholder en rekke krav til informasjonssikkerheten i kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v).

1998
- **Sikkerhetsloven** (loven skal primært motvirke trusler mot rikets selvstendighet og sikkerhet, og har bl.a et omfattende kapittel og forskrift om informasjonssikkerhet).

2000
- **Personopplysningsloven** (loven skal ivareta personvern og hjemler personopplysningsforskriften som i kapittel 2 inneholder en omfattende regulering av informasjonssikkerhet).

2001
- **Lov om elektroniske signaturer** (som fastsette krav til kvalifiserte sertifikater mv).
- **Forvaltningsloven § 15 a** om sikker kommunikasjon med forvaltningen (loven hjemler forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften) og forskriften gir en rekke regler som gjelder informasjonsssikkerhet).

Det ser ut til å være flere problemer knyttet til denne (og annen) rettslig regulering av informasjonssikkerhet. Særlig er det grunn til å nevne:
- Regelverkene er i liten grad samordnet. Dette er særlig et problem fordi én og samme virksomhet kan være forpliktet til å følge 3 regelverk samtidig, og disse regelverkene har delvis overlappende krav.

- Regelverkene er i stor grad så generelt formulert at de gir lite veiledning med hensyn til nærmere innhold og fremgangsmåter i sikkerhetsarbeidet. Dette er delvis utslag av at flere regelverk har meget vidt virkeområde, noe som gjør det nødvendig med et høyt generalitetsnivå.
- I sikkerhetsregelverkene vises det delvis til norske og internasjonale standarder, men disse har en uklar status og funksjon.

Det er åpenbart behov for forskning som foretar sammenlignende drøftelser av de aktuelle regelverkene. Særlig er det behov for forskning som evner å bearbeide hele feltet innenfor rammene av ett arbeid, for på den måten å skaffe oversikt over den totale innsatsen innen regulering av informasjonssikkerhet. Dette vil kreve en annen tilnærming enn hva en tradisjonell rettsdogmatisk studie vil representere. Således er det behov for "rettskildestudier" der det blir lagt vekt på å kartlegge det enkelte regelverkets regulatoriske strategi, regelstruktur, begrepsbruk, detaljeringsnivå mv, for deretter å sammenligne og drøfte disse generelle kjennetegnene nærmere. Bak en slik analyse må det ligge begrunnede standpunkter om hva som kan sies å være viktige kvalitetskrav til lovgivning og rettslig regulering ellers.

Forskningen om styring av informasjonssikkerhet bør ikke begrenses til det rettslige. Det er viktig å se rettslig regulering som et (viktig) eksempel på en styringsteknikk, og være oppmerksom på at det også finnes en rekke andre styringsteknikker. I mange tilfelle vil det være hensiktsmessig å gruppere de aktuelle styringsteknikkene som myndigheter har til rådighet i fem kategorier:

- Rettslige virkemidler (lov, forskrift, instruks, avtaler mv).
- Økonomiske virkemidler (bevilgninger, skatter, avgifter, etterspørsel som kunde mv).
- Organisatoriske virkemidler (endring av ytre organisatorisk struktur, instruksjons- og organisasjonsmyndighet, delegasjon og endret arbeidsdeling mv).
- Pedagogiske virkemidler (informasjonsarbeid, veiledning, konsulentvirksomhet, holdningskampanjer, bygging av "sikkerhetskultur" mv).
- Systemtekniske virkemidler (automatisering av sikkerhetsarbeidet, systemer for analyse og støtte til etterlevelse av rettslige og økonomiske krav mv).

De rettslige virkemidlene er på en måte i en særstilling, fordi de øvrige virkemidlene lett kan integreres i dem (loven fastsetter for eksempel organiseringen av sikkerhetsarbeidet). For forskere som primært har juridisk utdanning, er det også faglige grunner for spesielt å oppta seg med rettslige virkemidler. Selv om regelverket er forskerens "ståsted", er det imidlertid særlig viktig å belyse tre problemstillinger vedrørende *relasjonene* mellom rettslige og andre virkemidler:

1. I hvilken grad bør vi trekke annen virkemiddelbruk inn i de rettslige virkemidlene? – I hvilken grad bør vi for eksempel fastsette i loven hvordan organiseringen skal være, hvilke økonomiske incitamenter og hvilke krav som skal stilles til informasjonssystemene? Hva gir den beste styringsdyktighet i form av klarhet, fleksibilitet mv?
2. Hva bør balansen mellom ulike virkemidler være, og hvilken virkemiddelbruk er mest effektiv? Her er det ikke gitt at rettslige virkemidler alltid representerer den beste løsningen – i alle fall ikke alene. Særlig kan det være grunn til å spørre om nytten av å foreta rettslige reguleringer, uten samtidig å satse tungt på pedagogiske og systemtekniske tiltak som kan sikre at bestemmelsene blir kommunisert til de teknologiske miljøene som er regelverkets adressater.
3. Gitt en "arbeidsdeling" mellom rettslige og andre virkemidler – hvordan kan vi sørge for en helhetlig styring? Hvordan kan vi sikre tilstrekkelige sammenhenger mellom rettslig,

organisatorisk og økonomisk (mv) styring? Særlig kan det være grunn til å være oppmerksom på problemer som kan oppstå fordi tilsyn og sikkerhets-/forvaltningsrevisjon utføres av ulike profesjoner. Således kan det være grunn til å være skeptisk til ensidig dominans fra enkeltprofesjoner i arbeidet med informasjonssikkerhet. Normen bør trolig være tverrfaglige team som gjenspeiler hele bredden i den aktuelle virkemiddelbruken.

I undersøkelsen av rettslig regulering av informasjonssikkerhet og den totale virkemiddelbruken på området, inngår vurderinger av hva som er "effektivt", "hensiktsmessig" mv. Det er viktig at vi i forskningen ikke bare gjør løse normative antagelser om styringseffektene. Forskningen må i tillegg omfatte studier av implementering av regelverk og annen styring, for på den måten ha empirisk basis for å si noe om effekter. Her må vi holde mulighetene åpne for at det juristene mener er et "godt" regelverk, ikke er hensiktsmessig i det teknologiske miljøet som skal etterleve bestemmelsene.